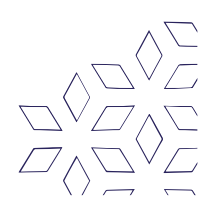


أكاديمية التعلم
Academy Of Learning
دبلوم الامن السيبراني
أساسيات الأمن السيبراني
تحت إشراف
المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

❖ الأهداف التفصيلية للمقرر

بنهاية هذا المقرر ستكون المتدربة قادرةً وبكفاءة على أن:

- يذكر مفهوم الأمن السيبراني ومصطلحات الأمن السيبراني
- يشارك في بناء استيراتيجيات الأمن السيبراني
- يحدث نظام التشغيل ويضبط إعداد الجدار الناري
- يثبت برامج مكافحة الفيروسات McAfee
- ينشئ حسابات أمنة طبقا للصلاحيات
- يجري نسخ احتياطي للملفات أو الكمبيوتر بالكامل
- يفسر مفهوم الاختراقات الأمنية والإجراءات اللازمة لتأمين الشبكات بمختلف أنواعها
- يوضح كيفية الاصطياد والهجوم الالكتروني وطرق الوقاية منها
- يطبق خطوات التصفح الأمن من خلال الإنترنت
- يبين وسائل الأمن المادي وأساليب أمن التقنيات المختلفة



❖ فهرس الكتاب

الفصل الأوّل: مقدمة في الأمن السيبراني

مفهوم الأمن السيبراني والهدف منه ٧

متطلبات وركائز الأمن السيبراني ٨

خطوات تحقيق الأمن السيبراني في المنظمات ١٠

أمن المعلومات والأمن السيبراني ١٢

أنماط التهديدات الأمنية وأبعاد أمن المعلومات ١٥

مفهوم الفضاء السيبراني ١٩

الحروب السيبرانية ٢١

المراحل الأساسية للأمن السيبراني ٢٢

جهود المملكة العربية السعودية في الأمن السيبراني ٢٤

الفصل الثاني: حماية الأنظمة واستراتيجيات الأمن السيبراني

مفهوم حماية الأنظمة ٢٦

أنظمة المعلومات ومكوناتها ٢٦

عناصر أمن المعلومات وتهديدات الأنظمة المعلوماتية ٢٨

العلاقة بين مستويات أمان المعلومات ٣٢

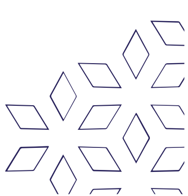
الأمان وعلاقته بالتكلفة أو بالزمن ٣٥

التخطيط الاستراتيجي للأمن السيبراني ٣٨

التصديق الرقمي ٤٥

أنظمة كشف التطفل ID ٤٧

الفصل الثالث: سياسات الأمن السيبراني ومعاييره



مفهوم السياسة الأمنية وأهميتها ٥٠

أنواع السياسات الأمنية ٥١

مفهوم المعايير القياسية وتصنيفها واستخدامها ٥٢

اللوائح والقوانين المتعلقة بالأمن السيبراني ٦٦

الأطراف المعنية بتنفيذ القواعد التي يجب الالتزام بها ٦٩

المعايير العالمية للأمن السيبراني ٧١

تصنيف المعلومات ومستوياتها ٧٩

التدريب والتوعية بالأمن السيبراني ٨٠

الفصل الرابع: أمن الحاسوب والبرمجيات

أمن الحاسوب ٨٢

أمن الملفات ٨٣

التهديدات الرقمية للحاسبات والبرمجيات (عملي) ٨٨

أمن أنظمة التشغيل ٨٩

مقارنة بين أنظمة التشغيل من حيث الأمان ٩٦

أنظمة حماية قواعد البيانات ٩٩

المخاطر الأمنية لنظم قواعد البيانات ١٠٣

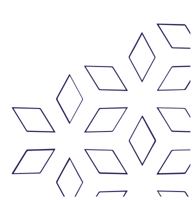
جدران الحماية وأنواعها ١٠٤

التهديدات الالكترونية الشائعة ١٠٩

الفصل الخامس: أمن الشبكات

مفهوم أمن الشبكات ١١٣

أهداف الحماية الأمنية للشبكات(عملي) ١١٤



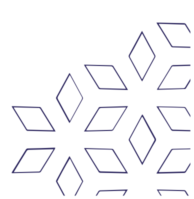
مفهوم الثغرات في أمن الشبكات ١١٥
التهديدات الرقمية لشبكات الحاسب ١١٦
أنواع الهجمات التي تتعرض لها الشبكة ١١٨
أمن الشبكات اللاسلكية(عملي) ١٢١
أمن وسائل نقل المعلومات(عملي) ١٢١
الشبكات المحلية الإفتراضية وأمنها ١٢٧
الاتصال الآمن بالإنترنت(عملي) ١٢٨
التدابير الأمنية العامة لأمن شبكات الحاسب ١٣٢

الفصل السادس: الهندسة الاجتماعية

مفهوم الهندسة الاجتماعية وأهدافها ١٣٦
أنواع الهندسة الاجتماعية ١٣٨
جوانب الهجمات بأسلوب الهندسة الاجتماعية ١٣٩
أساليب الهجوم باستخدام الهندسة الاجتماعية ١٤٠
الأثار المترتبة على الهندسة الاجتماعية ١٤١
إجراءات الحد من مخاطر الهندسة الاجتماعية ١٤٣
طرق رئيسية لحماية الأجهزة والمعلومات من الإختراق ١٤٧

الفصل السابع: الاصطياد والهجوم الالكتروني

نظام البريد الالكتروني ١٤٩
الاصطياد الالكتروني ١٥٣
التجسس الالكتروني ١٦٦
مفهوم الهجوم الالكتروني ١٧١



أنواع الهجوم الالكتروني ١٧٢

الفصل الثامن: أمن التعاملات الالكترونية

مفهوم التصفح الآمن ومميزاته ١٧٧

المخاطر التي تهدد المستخدم أثناء تصفح الإنترنت ١٧٩

خطوات التصفح الآمن من خلال الإنترنت ١٨٠

السياسيات الأمنية في المؤسسات الصحية ١٨٠

الأمان في مواقع التواصل الاجتماعي ١٨٢

حماية البيانات الشخصية في التجارة الالكترونية ١٨٦

التحقق الرقمي من الهوية ١٨٧

الفصل التاسع: وسائل الأمن المادي وأساليب أمن التقنيات المختلفة

مفهوم الأمن المادي وخصائصه ١٩١

أهمية الأمن المادي ١٩١

أنظمة الأمن المادي ١٩٢

الحماية المادية لمركز البيانات ١٩٩

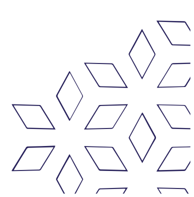
أمن البيانات الضخمة ٢٠٣

أمن الهواتف النقال ٢٠٥

المواطنة الرقمية ٢٠٦

الأمن الرقمي ٢٠٧

الاتصالات الرقمية ٢٠٨



أولاً: مقدمة في الامن السبراني

في هذا الفصل سنتعرف على المواضيع التالية:

- مفهوم الأمن السيبراني والهدف منه
- متطلبات وركائز الأمن السيبراني
- خطوات تحقيق الأمن السيبراني في المنظمات
- أمن المعلومات والأمن السيبراني
- أنماط التهديدات الأمنية وأبعاد أمن المعلومات
- مفهوم الفضاء السيبراني
- الحروب السيبرانية
- المراحل الأساسية للأمن السيبراني
- جهود المملكة العربية السعودية في الأمن السيبراني

❖ مفهوم الأمن السيبراني والهدف منه

يمكن تعريف الأمن السيبراني (بالإنجليزية) Cyber security بأنّه الأمن الذي يُعنى بتطبيق التقنيات، والعمليات، والضوابط بهدف حماية الأنظمة، وشبكات الحواسيب، والبرامج، والأجهزة، والبيانات من التعرض للهجمات الإلكترونية ويطلق عليه مسمى أمن تكنولوجيا المعلومات، أو أمن المعلومات الإلكترونية.

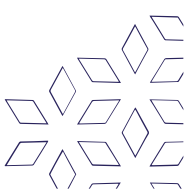
ويعرف ايضاً بانه: عملية حماية الأنظمة والشبكات والبرامج ضد الهجمات الرقمية، تهدف هذه الهجمات السيبرانية عادةً إلى الوصول إلى المعلومات الحساسة أو تغييرها أو تدميرها بغرض الاستيلاء على المال من المستخدمين أو مقاطعة عمليات الأعمال العادية.

يمثل تنفيذ تدابير الأمن السيبراني تحدياً كبيراً اليوم نظراً لوجود عدد أجهزة يفوق أعداد الأشخاص كما أصبح المهاجمون أكثر ابتكاراً.

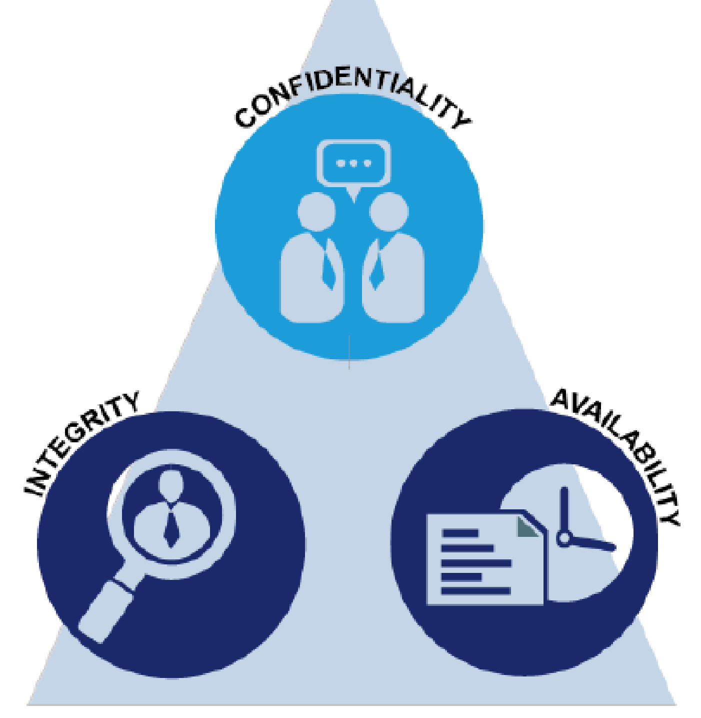
أهداف الأمن السيبراني

تكمن أهميّة الأمن السيبراني في عدة جوانب وفيما يأتي أبرزها:

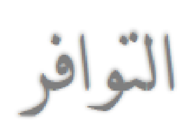
- يشمل كافة الأمور المرتبطة بحماية البيانات من المهاجمين المُختصين في سرقة المعلومات والتسبب بالضرر، إذ يمكن أن تكون هذه البيانات حساسة، أو معلومات حكومية وصناعية، أو معلومات شخصية، أو بيانات تعريف شخصية، أو حقوق ملكية فكرية.
- يُشكّل وجود برامج الأمن السيبراني وآليات الدفاع الإلكترونية وسيلة متطورة ذات أهمية كبيرة في حماية البيانات وخدمة مصلحة الجميع، إذ يعتمد جميع أفراد المجتمع على البُنية التحتية الحيوية كالمستشفيات، ومؤسسات الرعاية الصحية، وبرامج الخدمات المالية التي يجب المحافظة عليها.
- تقليل مخاطر الهجمات الإلكترونية على الصعيد الفردي، إذ يمكن أن تتسبب هذه الهجمات إلى تعرض الأفراد لسرقة هوياتهم وابتزازهم، وبالتالي إحداث أضرار وخيمة في حياة الأفراد.



اهداف الامن السيبراني







التوافر

❖ متطلبات وركائز الأمن السيبراني

يتطلب تطبيق الأمن السيبراني وجود سبع عناصر أساسية، وفيما يأتي توضيح لهذه العناصر:

الأشخاص:

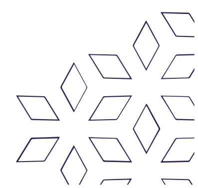
يمثّل هذا العنصر الأشخاص المعنيين بإدارة شبكة الأمن السيبراني، بحيث يجب أن يتوفر لديهم القدرة على التحقق من التهديدات الإلكترونية والدخول غير المصرّح به للأنظمة ومعالجتها، وتأمين الرد السريع للحوادث والهجمات.

السُلطة:

يجب تعيين شخص مسؤول عن تنفيذ عملية الأمن السيبراني، حيث يجب منحه النفوذ اللازم والصلاحيات للقيام بالتغيرات التنظيمية المطلوبة، وتطبيق برنامج الأمن السيبراني بسهولة.

الدعم من الإدارة العليا:

يجب الحصول على الدعم والتأييد من مجلس الإدارة، وفريق القيادة، وما يليه في التسلسل الإداري في الشركات، إذ يجب أن يتمتع برنامج الأمن السيبراني بالدعم التام لضمان نجاح تطبيقه.



العملية الفعّالة:

يجب أن يشتمل برنامج الأمن السيبراني على نهج فعّال يضمن إدارة عملية الأمن ومواجهة المخاطر الإلكترونية، بحيث يجب أن تحدد عملية الاستجابة للحوادث الإلكترونية الفعّالة كيفية استخدام الأشخاص للأدوات والتقنيات، وكيفية التصدي للهجمات الإلكترونية المُكتشفة.

التقنيات المناسبة:

يجب أن تكون التقنيات المُستخدمة في برنامج الأمن السيبراني قادرة على مواجهة ٧٥٪ من التهديدات المُكتشفة، والتحقيق فيما نسبته ٢٥٪ من التهديدات المحتملة، والتي تشكّل خطورة، وبالتالي يجب التحقق من صحتها من قِبل الأشخاص ذوي الخبرة.

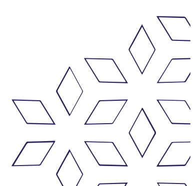
التواصل في الوقت المناسب:

تضمن عملية التواصل الداخلية في برنامج الأمن السيبراني والتي تحدث في الوقت المناسب نجاح برنامج الأمن، إذ يجب التنسيق بين فريق الأمن السيبراني وبين الجهات التي تتطلب الحماية من خلال مسؤولي الشبكات، ومهندسي الأنظمة، ومكتب المساعدة، والإدارة، وغيرهم.

الميزانية:

يتطلب نجاح برنامج الأمن السيبراني على المدى الطويل تخصيص ميزانية مناسبة له، والذي يعد أحد أهم عناصر الأمن السيبراني.





❖ خطوات تحقيق الأمن السيبراني في المنظمات

هناك عشر توصيات لتحقيق الامن السيبراني داخل المنظمات:

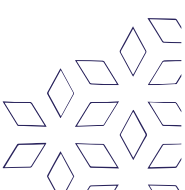
- تزويد جميع المستخدمين بمستويات تناسب أدوارهم والتحكم في منح امتيازات النظام وإدارتها.
- وضع استراتيجية لإزالة أو تعطيل الوظائف غير الضرورية لتجنب التضارب بين الأنظمة والمعلومات.
- التأكد من وجود نظام لإدارة المخاطر.
- تأمين الشبكة للحد من فرص تعرض الأنظمة للتهديد السيبراني.
- وضع سياسات وعمليات فاعلة لإدارة الحوادث الأمنية.
- رفع وعي وثقافة المستخدم عن كيفية حماية البيانات.
- التصدي للبرامج الضارة لتقليل المخاطرة عبر تطوير وتنفيذ سياسات مكافحة البرامج الضارة.
- إنشاء سياسات تدعم العمل المتنقل أو الوصول عن بعد إلى الأنظمة.
- الالتزام بضوابط الوسائل المتعددة القابلة للإزالة.
- المراقبة ومتابعة الأنظمة والكشف عن الهجمات الفعلية على الأنظمة والخدمات الإلكترونية.

<u>إدارة المخاطر</u>

أن الخطوة الأولى تتمثل في نظام إدارة المخاطر لتقييم المخاطر التي تتعرض لها معلومات وأنظمة المنظمة بتحديد نظام ملائم لإدارة المخاطر والتأكد من أن جميع منسـوبي المنظمة على علم تام بهذا النظام.

<u>التنظيم الآمن للمنظمة</u>

فيما تتركز الخطوة الثانية في التنظيم الآمن للمنظمة ويتم بها وضــع اســتراتيجية لإزالة أو تعطيل الوظائف غير الضرورية لتجنب التضارب بين الأنظمة والمعلومات.



تأمين الشبكات

تعتبر تأمين الشبكة هي الخطوة الثالثة لتحقيق الأمن السيبراني للحد من فرص تعرض الأنظمة للتهديد السيبراني، وبما أن الشبكات تغطي العديد من المواقع وتستخدم الاتصالات المتنقلة والخدمات السحابية، لذا يتطلب من المنظمات إنشاء وتنفيذ السياسات والاستجابات الهندسية والتقنية المناسبة التي تحمي شبكات المنظمة

إدارة صلاحيات المستخدم

تتمثل الخطوة الرابعة في إدارة صلاحيات المستخدم، فإذا تم تزويد المستخدمين بامتيازات نظام غير ضرورية أو حقوق وصول إلى البيانات، فإن ذلك يؤدي لزيادة خطر إساءة الاستخدام.

التثقيف الإلكتروني

الخطوة الخامسة تتلخص في وضع سياسات وعمليات فاعلة لإدارة الحوادث الأمنية.

رفع وعي وثقافة المستخدم

فيما تأتي الخطوة السادسة في رفع وعي وثقافة المستخدم عن كيفية حماية البيانات، إذ إن المستخدم يعتبر عاملا أساسيا في رفع مستوى الأمن المعلوماتي.

التصدي للمحتوى الضار

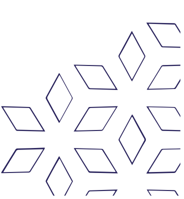
أن التصدي للبرامج الضارة هي الخطوة السابعة والمحققة للأمن السيبراني، وتتمثل في التصدي لأي كود أو محتوى له تأثير ضار وغير مرغوب فيه على الأنظمة، وأن أي تبادل للمعلومات يحمل في طياته درجة من المخاطرة وقد تؤثر على أنظمة المنظمة،

المراقبة ومتابعة الأنظمة

كما أن المراقبة ومتابعة الأنظمة والكشف عن الهجمات الفعلية على الأنظمة والخدمات الإلكترونية والتي تعتبر الخطوة الثامنة، أمر ضروري من أجل الاستجابة بفعالية للهجمات إضافة لإتاحتها لضمان استخدام الأنظمة بشكل مناسب وفقا للسياسات التنظيمية.

دعم العمل المتنقل

الخطوة التاسعة والعاشرة تتمثل في أهمية الالتزام بضوابط الوسائل المتعددة القابلة للإزالة، وسياسات ومراقبة العمل عن بعد، وذلك يعني إعداد سياسة للتحكم في الوصول إلى الوسائط القابلة للإزالة وهي وسائط التخزين الحاسوبية التي بالإمكان تنصيبها وإزالتها من الحاسوب والتي من المهم فحصها بحثا عن البرامج الضارة قبل استخدامها.



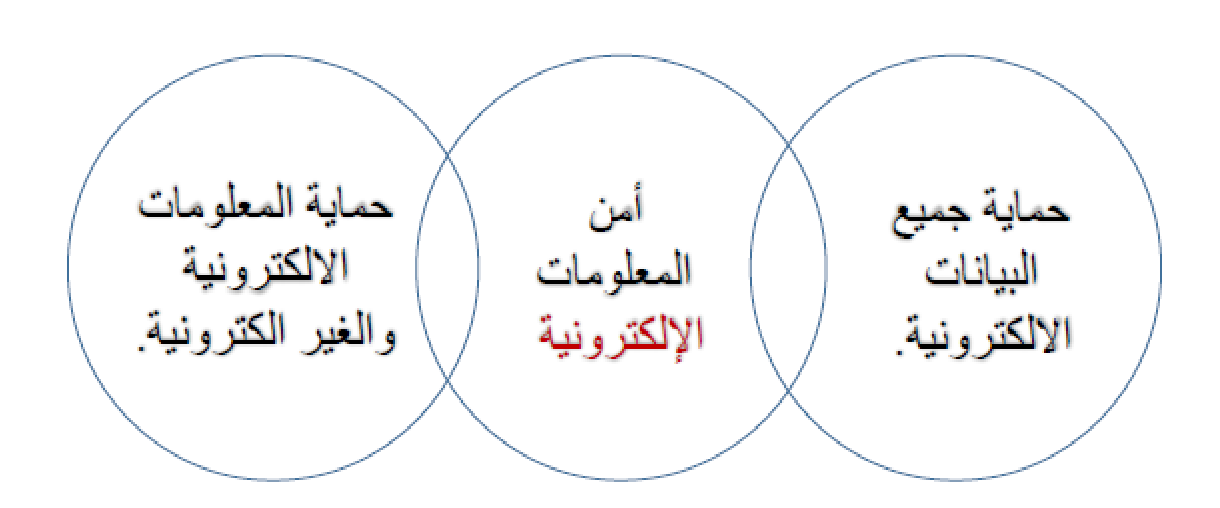
❖ أمن المعلومات والأمن السيبراني

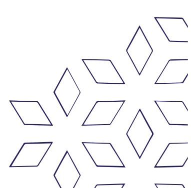
مفهوم أمن المعلومات

نشأ مفهوم أمن المعلومات فى بدايته عن طريق وكالة الاستخبارات المركزية الأمريكية (CIA)، بهدف حماية المعلومات من التهديدات والمخاطر التي من الممكن التعرض لها، كما يمكننا تعريفه على أنه العلم المختص بحماية وتأمين المعلومات الالكترونية عن طريق عدة أدوات واستراتيجيات تتبعها الدولة لضمان أمن وسلامة وسرية المعلومات الخاصة بها.

امن المعلومات: حماية الأنظمة الحاسوبية من الوصول غير الشرعي لها، او العبث المعلومات اثناء التخزين او المعالجة او النقل، والحفاظ على المعلومات وسريتها وتشفيرها بجميع اشكالها.

الامن السيبراني: فالأمن السيبراني يعتني بأمن كل ما يوجد ف الفضاء المعلوماتي ومن ضمنه "أمن المعلومات الرقمية".





الفرق بين الأمن السيبراني وأمن المعلومات

يُدرج في الجدول الآتي الفرق بين الأمن السيبراني، وأمن المعلومات:

الامن السيبراني	امن المعلومات
يسعى إلى حماية البيانات، ومصادر التخزين، والأجهزة من مخاطر الهجمات الإلكترونية في الفضاء السيبراني .	يسعى إلى حماية البيانات من أي نوع من أنواع التهديدات سواء كانت رقمية أم تناظرية أو قياسية
يتعامل مع الجرائم الإلكترونية، والاحتيال الإلكتروني، وتنفيذ القانون.	يتعامل مع عملية الوصول غير المصرّح به، والكشف عن أي تعديل أو خلل .
يعتمد تطبيق الأمن السيبراني على وجود أشخاص محترفين ومدربيّن على التعامل مع التهديدات وبالأخص تهديدات (APT) المتقدمة.	يوفّر أمن المعلومات قاعدة أساس لأمن البيانات، ويتم من خلاله تدريب الأشخاص على تحديد أولويات الموارد قبل مواجهة التهديدات أو الهجمات.

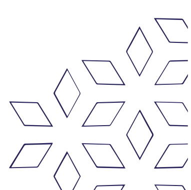
تهديدات أمن المعلومات

الفيروسات

تعتبر من أهم تهديدات أمن المعلومات فهي عبارة عن برامج مكتوبة بإحدى لغات البرمجة، الهدف منها هو إلحاق الضرر بالمعلومات الموجودة في الحاسوب، ولها ٣ خواص وهي التخفي والتضاعف وإلحاق الأذى، حيث إنه لا بد أن يكون مختفى داخل الجهاز وبمجرد إضافة الملف يتضاعف حجمه، كما انه يلحق الاذى بهذه الملفات أو بجهاز الحاسوب ككل.

اختراق المعلومات المرسلة

تحدث عن طريق اختراق شبكة معلوماتية معينة ومراقبة ما يحدث عليها او عن طريق اختراق حساب شخصي ومتابعة الرسائل التي تنتقل منه أو إليه مما يهدد أمن هذه المعلومات المرسلة وسهولة التجسس على الهيئات والمؤسسات وليس الأشخاص فحسب.



تهديد التجسس

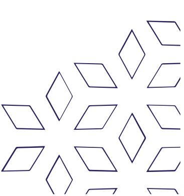
يعتبر واحد من أهم تهديدات أمن المعلومات حيث إنه لا يصيب الضرر بالجهاز، فمن الممكن ألا يتم التعرف عليه أو اكتشافه لأنه يقتصر على مراقبة الجهاز ومتابعة معلوماته دون إلحاق ضرر به، وهو من أخطر التهديدات لأمن وسرية المعلومات السياسية أو الشخصية وغيرها.

السيطرة الكاملة

يحدث هذا التهديد عن طريق إرسال ملف صغير من قبل المخترق إلى جهاز الضحية عبر أحد الرسائل مثلاً أو يقوم بإرسال رابط يحتوي على فيروس يمكنه من مراقبة جهاز المستخدم ومتابعة تفاصيلها، وبامكانه من خلال هذا التهديد أيضاً تعطيل أحد الخدمات على جهاز المستهدف مما يعيق تعامله بحرية على جهازه.

هجوم التضليل

يحدث هذا الهجوم أو التهديد عن طريق انتحال موقع موثوق أو شخصية ما موثوقة، حتى يتمكن المخترق من خلالها من الحصول على معلومات الحسابات الشخصية أو غيرها من المعلومات السرية والحساسة.



❖ أنماط التهديدات الأمنية وأبعاد أمن المعلومات

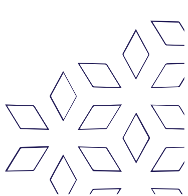
تتراوح التهديدات الأمنية الشائعة من التهديدات الداخلية إلى التهديدات المستمرة المتقدمة، ويمكنها أن تسبب الخسائر ما لم يكن فريق الأمن الداخلي على علم بها ومستعد للرد، حيث إن التهديد الأمني هو عمل خبيث يهدف إلى إفساد، أو سرقة البيانات، أو تعطيل أنظمة المؤسسة ،أو المنظمة بأكملها، والحدث الذي ينتج عنه خرق للبيانات أو الشبكة يسمى الحادث الأمني، **أهم ١٠ أنواع من تهديدات أمن المعلومات:**

١. التهديدات الداخلية:

يحدث التهديد من الداخل عندما يسيء الأفراد المقربون من مؤسسة ما الذين أذن بالوصول إلى شبكتها عن قصد أو عن غير قصد استخدام هذا الوصول للتأثير سلباً على البيانات أو الأنظمة المهمة للمؤسسة، الموظفون المهملون الذين لا يمتثلون لقواعد وسياسات عمل مؤسساتهم يتسببون في تهديدات داخلية، على سبيل المثال، قد يرسلون بيانات العملاء عبر البريد الإلكتروني عن غير قصد إلى أطراف خارجية، أو ينقرون على روابط التصيد الاحتيالي في رسائل البريد الإلكتروني أو يشاركون معلومات تسجيل الدخول الخاصة بهم مع الآخرين، كما أن المقاولون وشركاء الأعمال والموردون الخارجيون هم مصدر التهديدات الداخلية الأخرى، يتجاهل بعض المطلعين عمداً الإجراءات الأمنية بدافع الملاءمة أو محاولات غير مدروسة ليصبحوا أكثر إنتاجية، ويتهرب المطلعون الضارون عمداً من بروتوكولات الأمن السيبراني لحذف البيانات أو سرقة البيانات لبيعها أو استغلالها لاحقاً أو تعطيل العمليات أو إلحاق الضرر بالنشاط التجاري.

٢. الفيروسات والديدان:

الفيروسات والديدان هي برامج ضارة تهدف إلى تدمير أنظمة وبيانات وشبكات المؤسسة، حيث إن فيروس الكمبيوتر هو رمز ضار يتكرر عن طريق نسخ نفسه إلى برنامج أو نظام أو ملف مضيف آخر، ويظل كامناً حتى يقوم شخص ما بتنشيطه عن قصد أو عن غير قصد، وينشر العدوى دون علم أو إذن من المستخدم أو إدارة النظام، بينما دودة الكمبيوتر هي برنامج يتكاثر ذاتيًا ولا يحتاج إلى نسخ نفسه إلى برنامج مضيف أو يتطلب تفاعلاً بشرياً للانتشار، وتتمثل مهمتها الرئيسية في إصابة أجهزة الكمبيوتر الأخرى مع استمرار نشاطها على النظام المصاب، وغالباً ما تنتشر الديدان باستخدام أجزاء من نظام التشغيل تكون تلقائية وغير مرئية للمستخدم، وبمجرد دخول الدودة إلى النظام، فإنها تبدأ على الفور في تكرار نفسها، ممّا يؤدي إلى إصابة أجهزة الكمبيوتر والشبكات غير المحمية بشكل كافٍ.

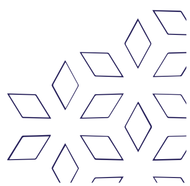


٣. بوت نت:

وتسمى الروبوتات وهي عبارة عن مجموعة من الأجهزة المتصلة بالإنترنت، بما في ذلك أجهزة الكمبيوتر والأجهزة المحمولة والخوادم وأجهزة تقنيات عمليات التي تقوم إصابة وعن بعد التي تسيطر عليها نوع شائع من البرامج الضارة، وعادةً ما تبحث برامج الروبوتات الضارة عن الأجهزة المعرضة للخطر عبر الإنترنت، الهدف من إنشاء عامل التهديد الذي ينشئ شبكة الروبوتات هو إصابة أكبر عدد ممكن من الأجهزة المتصلة، باستخدام قوة الحوسبة وموارد تلك الأجهزة للمهام الآلية التي تظل مخفية عموماً لمستخدمي الأجهزة، ويستخدمها الفاعلون المهددون – غالباً مجرمو الإنترنت – الذين يتحكمون في شبكات الروبوت هذه لإرسال بريد إلكتروني عشوائي والمشاركة في حملات النقر الاحتيالية وإنشاء حركة مرور ضارة لهجمات رفض الخدمة الموزعة.

٤. هجمات التنزيل:

في هجوم التنزيل من محرك الأقراص، يتم تنزيل التعليمات البرمجية الضارة من موقع ويب عبر متصفح أو تطبيق أو نظام تشغيل متكامل دون إذن المستخدم أو علمه، ولا يتعين على المستخدم النقر فوق أي شيء لتنشيط التنزيل، مجرد الوصول إلى موقع الويب أو تصفحه يمكن أن يبدأ التنزيل، ويمكن لمجرمي الإنترنت استخدام التنزيلات من خلال محرك الأقراص لضخ أحصنة طروادة المصرفية وسرقة المعلومات الشخصية وجمعها بالإضافة إلى تقديم مجموعات استغلال أو برامج ضارة أخرى إلى نقاط النهاية.



٥. هجمات التصيد:

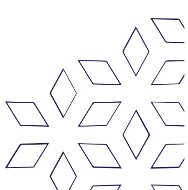
تعد هجمات التصيد الاحتيالي نوعاً من تهديد أمن المعلومات الذي يستخدم الهندسة الاجتماعية لخداع المستخدمين لكسر ممارسات الأمان العادية والتخلي عن المعلومات السرية، بما في ذلك الأسماء والعناوين وبيانات اعتماد تسجيل الدخول وأرقام الضمان الاجتماعي ومعلومات بطاقة الائتمان والمعلومات المالية الأخرى، وفي معظم الحالات، يرسل المتسللون رسائل بريد إلكتروني مزيفة تبدو وكأنها قادمة من مصادر مشروعة، مثل المؤسسات المالية و (eBay) و (PayPal) وحتى الأصدقاء والزملاء، في هجمات التصيد الاحتيالي، يحاول المتسللون حمل المستخدمين على اتخاذ بعض الإجراءات الموصى بها، مثل النقر على الروابط في رسائل البريد الإلكتروني التي تنقلهم إلى مواقع ويب احتيالية تطلب معلومات شخصية أو تثبيت برامج ضارة على أجهزتهم، ويمكن أن يؤدي فتح المرفقات في رسائل البريد الإلكتروني أيضاً، إلى تثبيت برامج ضارة على أجهزة المستخدمين المصممة لجمع المعلومات الحساسة أو إرسال رسائل البريد الإلكتروني إلى جهات الاتصال الخاصة بهم أو توفير الوصول عن بُعد إلى أجهزتهم.

٦. هجمات حجب الخدمة الموزعة:

في هجوم رفض الخدمة الموزع (DDoS) ، تهاجم العديد من الأجهزة المخترقة هدفاً، مثل خادم أو موقع ويب أو مصدر شبكة آخر، ممّا يجعل الهدف غير قابل للتشغيل تماماً، وقد يجبر تدفق طلبات الاتصال أو الرسائل الواردة أو الحزم المشوهة النظام المستهدف على الإبطاء أو التعطل والإغلاق، ممّا يحرم المستخدمين أو الأنظمة الشرعية من الخدمة.

٧.برامج الفدية:

في هجوم برامج الفدية، يتم قفل كمبيوتر الضحية، عادةً عن طريق التشفير، ممّا يمنع الضحية من استخدام الجهاز أو البيانات المخزنة عليه، ولاستعادة الوصول إلى الجهاز أو البيانات، يتعين على الضحية دفع فدية للمتسلل، عادةً بعملة افتراضية مثل (Bitcoin) يمكن أن تنتشر برامج الفدية عبر مرفقات البريد الإلكتروني الضارة وتطبيقات البرامج المصابة وأجهزة التخزين الخارجية المصابة ومواقع الويب المخترقة.



٨. مجموعات استغلال:

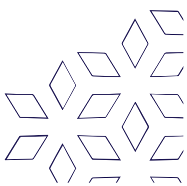
هي أداة برمجة تسمح للشخص من دون أي خبرة كتابة التعليمات البرمجية البرمجيات لإنشاء وتخصيص وتوزيع البرامج الضارة، ومن المعروف أن مجموعات استغلال من جانب مجموعة متنوعة من الأسماء، بما في ذلك عدة العدوى، مجموعة برمجيات الجريمة وأدوات البرمجيات الخبيثة، ويستخدم مجرمو الإنترنت مجموعات الأدوات هذه لمهاجمة نقاط الضعف في النظام لتوزيع البرامج الضارة أو الانخراط في أنشطة ضارة أخرى، مثل سرقة بيانات الشركة أو شن هجمات رفض الخدمة أو بناء شبكات الروبوت.

٩. هجمات التهديد المستمر المتقدمة:

التهديد المستمر المتقدم (APT) هو هجوم إلكتروني مستهدف يخترق فيه متطفل غير مصرح به شبكة ويظل غير مكتشفة لفترة طويلة من الزمن. بدلاً من التسبب في تلف نظام أو شبكة، فإن الهدف من هجوم (APT) هو مراقبة نشاط الشبكة وسرقة المعلومات الوصول، بما في ذلك مجموعات الاستغلال والبرامج الضارة. وعادةً ما يستخدم مجرمو الإنترنت هجمات (APT) لاستهداف أهداف عالية القيمة، مثل الشركات الكبيرة والدول القومية، لسرقة البيانات على مدى فترة طويلة.

١٠. هجوم:(Malvertising)

وهي تقنية يستخدمها مجرمو الإنترنت لإدخال تعليمات برمجية ضارة في شبكات الإعلانات وأيضاً في صفحات الويب المشروعة عبر الإنترنت.



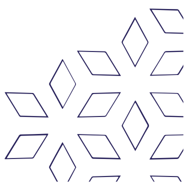
❖ مفهوم الفضاء السيبراني

يُعرّف الفضاء السيبراني:Cyperspace بأنه عالم الحاسوب الافتراضي، أو الوسيلة الإلكترونية المُستخدمة لتسهيل التواصل عبر شبكة الإنترنت، ويشمل الفضاء السيبراني شبكة حاسوب كبيرة مكونة من عدّة شبكات حاسوب فرعية منتشرة في جميع أنحاء العالم

يعتمد الفضاء السيبراني على بروتوكولTCP /IP ؛ لتسهيل تبادل البيانات والملفات، والتواصل بفاعلية بين مجموعة كبيرة من المستخدمين، وتتيح لهم تبادل المعلومات والأفكار؛ والمشاركة في مُختلف المناقشات؛ أو المنتديات الاجتماعية؛ وممارسة الألعاب؛ من خلال وسائط سهلة الاستخدام، وغيرها الكثير من الخدمات.

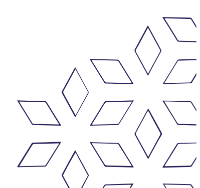
الفرق بين الفضاء السيبراني والإنترنت

قد يخلط البعض بين مفهومي الفضاء السيبراني والإنترنت، ويعتقدون أنّهما يعبّران عن نفس المفهوم، وهو أمر غير صحيح؛ فالإنترنت إحدى الشبكات العالمية التي تنشأ من خلال ربط شبكات أصغر من الحواسيب والخوادم، بينما الفضاء السيبراني حيّز رمزي أو افتراضي يوجد ضمن نطاق الإنترنت. ومرّة أخرى، قد يخطئ البعض في الاعتقاد أنّ كلاً منهما نظام مختلف تماماً في عالم التكنولوجيا، وأنه لايوجد ترابط بينهما، بينما الحقيقة وجود ترابط وثيق بينهما؛ نظراً لوجود الفضاء السيبراني داخل نطاق شبكة الإنترنت، وإنجاز جميع العمليات داخل حيّزه عن طريق شبكة الإنترنت، مثل: إرسال البريد الإلكتروني، أو فتح مواقع الويب.



نشأة وتطور الفضاء السيبراني

ظهر مصطلح الفضاء السيبراني لأول مرّة في عام ١٩٨٢م، من قِبَل المؤلف الأمريكي الكندي ويليام جيبسون، في رواية الخيال العلمي (نيورومانسر)، وبالتالي فإنّ نشأته تعود لفترة التسعينيات من القرن الماضي، بعد ظهور شبكة الإنترنت؛ لدعم عمليات التواصل والتفاعل بين الأفراد، خاصةً بعد انتشار غرف الدردشة، والمحادثات الجماعية. كما يعد الفضاء السيبراني داعمًا أساسيًا للمراسلات عبر البريد الإلكتروني، والوصول إلى الألعاب الإلكترونية، واستمرارية استخدام شبكات الإنترنت وتطورها أثّر على تطوّر الفضاء السيبراني ليواكب التحديثات القائمة على طرق التواصل، من خلال تسهيل إقامة مدونات، وغرف للدردشة، والمدونات الشخصية، دون الحاجة لتعلّم برمجة البرامج، وقد أدى ذلك لإتاحة الفرص لمزيد من الأفراد الراغبين بإنشاء مواقع مناقشات عامة في الفضاء السيبراني عبر شبكة الإنترنت، لكن في أولى مراحل تطوّر الإنترنت في منتصف التسعينيات، عبّر الكثير من المستخدمين عن ضرورة إلغاء تحكّم الجهات الحكومية الوطنية في الفضاء السيبراني؛ كنوع من حرية التعبير للمستخدمين. إلّا أن الحكومات الوطنية أظهرت ضرورة وجود لوائح وطنية، واتفاقات دولية خاصة بالفضاء السيبراني؛ لحماية حقوق المستخدمين، والوصول لجميع الهويات التي تسعى لتنفيذ الجرائم الإلكترونية، ومنع انتهاك خصوصية جميع المستخدمين، لذا لابُد من وضع بعض القيود، وتحديث بنية الفضاء السيبراني باستمرار حتى هذا اليوم.



❖ الحروب السيبرانية

ما هي الحرب السيبرانية؟ وما مدى خطورتها؟

في ظل التطور التكنولوجي الهائل الحاصل في العالم من حولنا. ومع المزايا التي لا تعد ولا تحصى لهذا التطور، ولكن هل رأينا الوجه الآخر لهذا التطور المهول! وهو ما يمكننا سميته ب الحرب السيبرانية!

ف ما هي الحرب السيبرانية؟ وما مدى معرفتنا لحجم خطورتها على العالم وعلينا كأفراد،

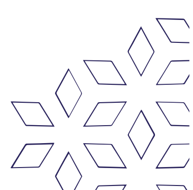
يمكننا أن نعتبر الحرب السيبرانية احدى أخطر الحروب الإلكترونية التي يمر بها العالم الحديث، وأكثرها دماراً، ويرتبط مدى حماية المجتمع والأفراد على حدٍ سواء من خطورتها، بضرورة التوعية لأهمية تحسين الأمن السيبراني ومعرفتهم له، في ظل استخدام الأفراد غير المنقطع للتكنولوجيا وللإنترنت، سواء على الصعيد الشخصي أو العملي.

مفهوم الحرب السيبرانية

تميز التاريخ العالمي للحروب بوجود حرب تميز كل حقبة زمنية وتعتبر الأعظم في تلك الحقبة، فكانت على مر العصور والسنوات حروب ميزت كل عصر، بدءاً من الحروب التقليدية وصولاً للحروب الكيماوية والنووية.

وفي ظل ما شهده العالم من تطور علمي وتكنولوجي كبير، اتجه العالم نحو نوع جديد من الحروب وهي الحرب السيبرانية وتعد من أعظم الحروب، بل وأشدها فتكاً، نظراً لكونها مجهولة الجهات التي تقوم بها، فمثلاً: قد تتعرض الدول لهجوم سيبراني فلا تعرف الفاعل، ولا تعلم به الا بعد حدوثه!

ويرتبط مفهوم الحرب السيبرانية بانه عبارة عن هجمات الكترونية بقيادة عسكرية تقوم باختراق الأنظمة الالكترونية العالمية وكل ما يعتمد على التكنولوجيا، لتضر بالحواسيب والأجهزة التي تستخدم شبكة الانترنت العالمية والتي قد تفضي لنتائج كارثية، مثل سرقة بيانات خاصة، وغيرها من الكوارث التي قد تكون عالمية مثل الحروب النووية وغيرها.



تاريخ الحرب السيبرانية

يمكننا القول بأن اول استخدام لمصطلح" السيبرانية" قد كان في الربع الأول من النصف الثاني من القرن الماضي، والذي ذكره الكاتبان كلاينس وكلاين في مقالاتهم للإشارة بين الانسان والالكترونيات معاً، وبعد ذلك كان مدى استخدام هذا المصطلح ضئيل الى حدٍ ما.

وفي عام ١٩٨٣ أصدرت هوليود فيل" العاب الحرب" " War Games" والذي يروى قصة فتى هاوي وعبقري في الحاسوب،بحيث يستطيع ان يخترق الجهاز الرئيسي للجيش الأمريكي، مسبباً بذللك ازمة عالمية كادت ان تنتهي بحرب عالمية ثالثة، كان هذا الفيلم بمثابة شرارة التي دفعت بالكثيرين ليتساءلوا تجاه إمكانية تحقيق ما جاء بالفلم فعلياً، وهل هو مستحيل ام لا! ولم يدركوا ان الأمر قد يكون بمثابة عرض بسيط لما سيحدث لاحقاً بفعل الحرب السيبرانية التي ستغزو العالم أجمع!

❖ المراحل الأساسية للأمن السيبراني

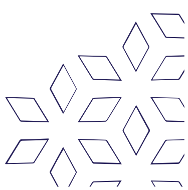
أنواع ومراحل الأمن السيبراني يُصنف الأمن السيبراني إلى عدة أنواع، وفيما يأتي أشهرها:

أمن الشبكة:

يُعنى أمن الشبكة بتوفير الحماية لشبكة الكمبيوتر من تهديدات المتطفلين، وتكون هذه التهديدات إما من المهاجمين المُستهدفين أو من البرامج الانتهازية الضارّة.

أمن التطبيقات:

يهتم أمن التطبيقات بإبقاء البرمجيات، والأجهزة دون أي تهديدات، إذ يمكن أن يسهّل التطبيق المُخترق إمكانية الوصول إلى البيانات التي صُممّت لتأمين الحماية، وبالتالي فإنَّ برنامج الأمن الناجح يبدأ في مرحلة التصميم الأوليّة، أي قبل نشر البرامج أو الأجهزة، أمن المعلومات يركّز أمن المعلومات على تأمين الحماية لسلامة البيانات وخصوصيتها، وذلك أثناء عملية تخزينها، أو أثناء عملية تناقلها.



الأمن التشغيلي:

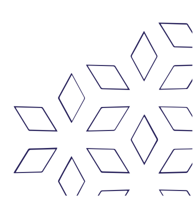
يندرج تحت مظلة الأمن التشغيلي العمليات والقرارات المرتبطة بمعالجة أصول البيانات وحمايتها، بالإضافة إلى الأذونات التي يحتاج لها المستخدمين للوصول إلى الشبكة، والإجراءات الخاصة بكيفية ومكان تخزين البيانات أو مشاركتها.

الاسترداد بعد الكوارث واستمرارية الأعمال:

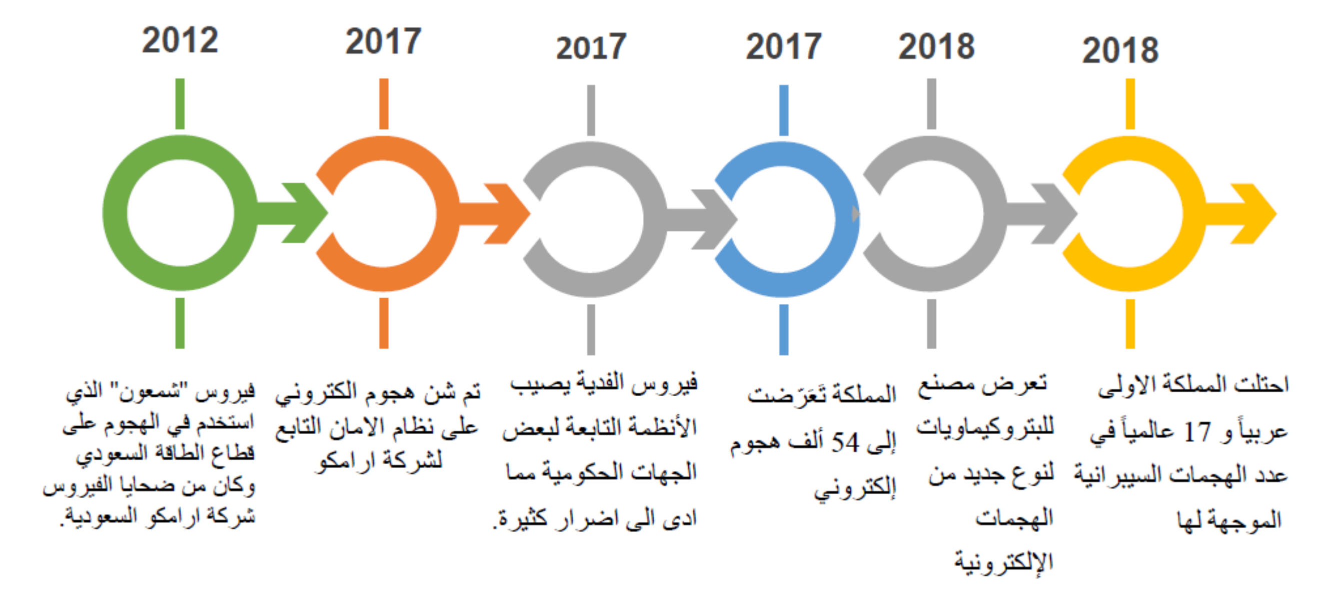
يهتم هذا النوع من الأمن بتحديد الكيفية المتبّعة في استجابة المنظّمة لحادث أمن سيبراني أو أي حدث آخر يؤدي إلى فقدان العمليات أو البيانات، إذ تضع سياسات التعافي من الكوارث طرق استرداد المؤسسة لعملياتها ومعلوماتها بهدف استمرارية العمل.

تعليم أو تثقيف المستخدم الجديد:

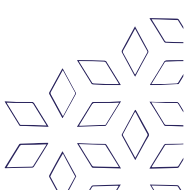
يجب الأخذ بعين الاعتبار تعليم الأشخاص، إذ يمكن أن يتسبّب أي شخص دون قصد بإدخال أحد الفيروسات إلى نظام الأمن نتيجة عدم اتبّاع ممارسات الأمن الصحيحة، بحيث تعد عملية تعليم المستخدمين لآلية حذف مرفقات رسائل البريد الإلكتروني المشبوهة، وعدم توصيل محركات الأقراص مجهولة المصدرUSB وغيرها من أهم الأمور الواجب تعلّمها.



❖ جهود المملكة العربية السعودية في الأمن السيبراني



- تم تشكيل الهيئة الوطنية للأمن السيبراني October 31, 2017 لرفع مستوى الحماية للشبكات C والاجهزة والأنظمة المعلوماتية وما تحويه من بيانات.
- تم إنشاء لاتحاد السعودي للأمن السيبراني والبرمجة والدرونز.
- تم إنشاء مركز الأمن الإلكتروني لمواجهة التهديدات الالكترونية موجهة على المملكة العربية السعودية.
- إنشاء كلية متخصصة بالأمن السيبراني والبرمجة والذكاء الاصطناعي تسعى إلى بناء وتأهيل قدرات وطنية شابة محترفة للمساهمة في تحقيق اهداف المملكة في رؤية ٢٠٣٠.
- وزارة التعليم والهيئة الوطنية للأمن السيبراني قامت بتخصيص ١٠٠٠ مقعد للمستفيدين والمستفيدات من برنامج خادم الحرمين الشريفين للإبتعاث الخارجي في مجال الأمن السيبراني.
- العديد من الجامعات السعودية تضمن مجاليا لذكاءالاصطناعي والأمن السيبراني في خططها.
- وضع الاستراتيجية الوطنية للأمن السيبراني الجديدة من قبل الهيئة الوطنية للأمن السيبراني.



ثانياً: حماية الأنظمة واستيراتيجيات الأمن السيبراني

في هذا الفصل سنتعرف على المواضيع التالية:

- مفهوم حماية الأنظمة
- أنظمة المعلومات ومكوناتها
- عناصر أمن المعلومات وتهديدات الأنظمة المعلوماتية
- العلاقة بين مستويات أمان المعلومات
- الأمان وعلاقته بالتكلفة أو بالزمن
- التخطيط الاستيراتيجي للأمن السيبراني
- التصديق الرقمي
- أنظمة كشف التطفل IDS

❖ مفهوم حماية الأنظمة

مع تطور التكنولوجيا ووسائل تخزين المعلومات وتبادلها بطرق مختلفة أو ما يسمى نقل البيانات عبر الشبكة من موقع لآخر أصبح أمر أمن تلك البيانات والمعلومات يشكل هاجساً وموضوعاً حيويًا مهمًا للغاية.

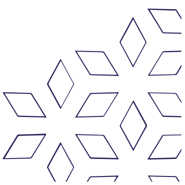
نحن اليوم بحاجة إلى الحماية أكثر من أي وقت مضى، خاصة عند الحديث عن العالم الالكتروني والشبكة العنكبوتية التي يؤثر اختراقها على كل نواحي الحياة بالنسبة لنا، والتي من الممكن ان يتضرر الجانب النفسي والمادي والعملي لدينا في حال تم تسريب اي من محتوانا الخاص او بياناتنا الشخصية المرفقة والمحفوظة على منصاتنا الشخصية على الانترنت.

ويمكن تعريف مفهوم حماية الأنظمة بأنه علم مختص بتأمين المعلومات المتداولة عبر شبكة الانترنت من المخاطر التي تهددها، أو الحاجز الذي يمنع الاعتداء عليها وذلك من خلال توفير الأدوات والوسائل اللازم توفيرها لحماية المعلومات من المخاطر الداخلية أو الخارجية، المعايير والإجراءات المتخذة لمنع وصول المعلومات إلى أيدي أشخاص غير مخوّلين عبر الاتصالات ولضمان أصالة وصحة هذه الاتصالات.

❖ أنظمة المعلومات ومكوناتها

١- **<u>المكونات المادية:</u>**

يساهم وجود الأجهزة في تحقيق السرعة لنظم المعلومات، والدقة والسعة التي تحتاجها، لوجود كميّات هائلة من البيانات، وتضمّ المكونات المادية أجهزة الملحقات الطرفية كأجهزة الإدخال والاخراج، وأجهزة التخزين الثانوية، والمعالجات والذاكرة الرئيسية، بحيث يتمّ قبول البرامج والبيانات وتخزينها ومعالجتها من خلال التعليمات وإعطاء النتائج.



٢- المكونات البرمجية:

تشمل المكونات البرمجية (Computer software) ما يأتي:

- **برنامج النظام:** وهي أنظمة التشـغيل، مهمتها تقديم الدعم والتحكّم في عمليات نظام الكمبيوتر.
- **برامج التطبيقات:** تهـدف هـذه البرامج لتوجيه أجهزة معينة للعمل بها من المسـتخـدم النهائيّ، مثل: برنامج تحليل المبيعات، وبرنامج الرواتب.
- **الإجراءات:** هي التعليمات الخاصة، حيث يعمل عليها ممّن يستخدمون نظام المعلومات فأما أن تكون هذه الإجراءات على شكل نموذج ورقيّ أو برنامج حاسوبيّ.

٣- البيانات:

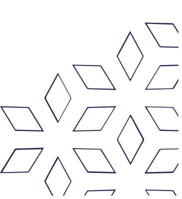
قواعد البيانات ومستودعات البيانات قواعد للبيانات (Databases) هي مستودع المادة الأساسية التي تعمل بها المكونات الأخرى، وتعدّ مجمع البيانات التي تسترجع من خلال الاستعلام عنها حسب ضوابط محددة، في حين أنّ مستودع البيانات data warehouses تشمل جميع البيانات بأي شكل تحتاجه المؤسسة وقد برزت أهميتها في أنظمة المعلومات مع وجود البيانات الضخمة، حيث توجد بيانات هائلة من الممكن جمعها وتحليلها.

٤- افراد والاجراءات:

الموارد البشرية والإجراءات يلعب قسم الموارد البشرية (Human resources and procedures) دوراً مهماً، ويرجع السبب في ذلك إلى أنّ جميع مكوّنات نظم المعلومات لا يمكن تشغيلها ووضع الإجراءات اللازمة لإدخالها، تخزينها وتحليلها دون وجود العنصر البشريّ الذي يحوّل هذه المعرفة لقواعد بيانات.

٥- الشبكات:

الاتصال عن بعد ترتبط الأجهزة في نظم المعلومات ببعضها من خلال اتصال سلكي، مثل كابلات الإيثرنت (Ethernet) والألياف البصرية، أو لاسلكية، مثل شبكة الواي فاي(Wi-Fi) ، إذ يمكن إنشاء شبكة تربط ما بين أجهزة الكمبيوتر كالتي توجد بالجامعات، مثل الشبكات المحلية (local area network).



❖ عناصر أمن المعلومات وتهديدات الأنظمة المعلوماتية

١- عناصر امن المعلومات

تسعى كافة وسائل أمن المعلومات لتحقيق الغاية الرئيسية المتمثلة في ضمان حماية المعلومات والمحافظة عليها، ان هدف الابحاث والاستراتيجيات ووسائل أمن المعلومات، **يتمثل في ضمان توفر ثلاثة عناصر رئيسية لأية معلومات، وهي:**

(١) سرية المعلومات confidentiality

تشمل كافة التدابير اللازمة لمنع اطلاع الجهات غير المصرح لها على المعلومات الحساسة او السرية.

(٢) تكامل وسلامة المعلومات Integrity

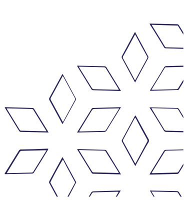
تشمل كافة التدابير اللازمة لحماية المعلومات من التغيير.

(٣) توفر المعلومات Availability

تشمل كافة التدابير اللازمة لضمان التأكد من استمرار القدرة على تقديم الخدمات والتفاعل مع المعلومات والوصول إليها.

(٤) عدم انكار التصرف المرتبط بالمعلومات ممن قام به Non - Reputation

ضمان عدم انكار الشخص انه قام بتصرف ما متصل بالمعلومات.



٢- تهديدات أمن المعلومات

تتزايد التهديدات التي تتعرض لها المنظمات نتيجة التطور المتسارع في الأساليب التي يمكن من خلالها الوصول لبيانات ومعلومات سرية خاصة بالمنظمة بشكل غير مصرح به بهدف تعديلها او سرقتها او حتى تدميرها .

يمكن تصنيف أساليب الاحتيال الالكتروني بهدف الحصول على المعلومات بأسلوب غير مصرح به الي ثلاث أساليب وهي :

(1)اختراق الشبكات :(Hacking)

ويقصد به الوصول غير المصرح به للشبكة او نظام المعلومات المحاسبي بهدف تعديل البيانات، او المعلومات، او سرقتها، او تدميرها.

ويحتوي هذا الأسلوب على عدة تقنيات منها كمثال لتقنيات شائعة في هذا المجال :

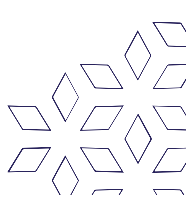
أ– سرقة كلمة السر :(Password Cracking)

اختراق الشبكة والاطلاع على المعلومات الخاصة بالشركة من خلال سرقة كلمة السر الخاصة بالمعنيين داخل الشركة .

ب– هجمات حقن قواعد البيانات :(structured Query Language Injection Attack)

مثلا من خلال إدخال برمجية ضارة مكان كلمة السر او اسم المستخدم إذ تمكن المحتال من الوصول إلى قواعد البيانات بهدف سرقتها أو التعديل فيها أو تدميرها .

ج– التعرض للإختراق أثناء محاولة معالجة اختراق سابق (Zero-day-attack)



(2)الهندسة الاجتماعية :

ويقصد بها تحفيز المستخدم على الإفصاح عن بيانات سرية من خلال طرح أسئلة بسيطة بهدف جمع معلومات دون إثارة شبهة .

ويحتوي هذا الأسلوب على عدة تقنيات منها :

أ- التوأمة الشريرة :(Evil Twin)

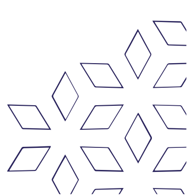
اي ادعاء جهة معينة بأنها جهة موثوق منها من قبل المستخدم تطلب منه استخدام ملف مرفق يكون ضاراً به .

ب- سرقة الهوية :(Identity Theft)

اي ادعاء جهة معينة بأنها جهة أخرى معروفة من قبل المستخدم، بحيث يتم الطلب منه تقديم المعلومات بشكل مباشر .

ج- التصيد :(phishing)

ويقصد منها وصول رسالة مزيفة من جهة (غالبا مالية ومعروفة) لطلب معلومات او التحقق منها، ولتحقيق ذلك قد تحتوي هذه الرسائل على رابط مزيف لجهة معروفة .



(3)البرمجيات الضارة :(Malware)

وهي عبارة عن برامج متخصصة لتسهيل التسلل الي النظام او الشبكة بهدف تدميرها، وما أن يتم تثبيت البرمجية الضارة فإنه من الصعب جدا إزالتها .

ويحتوي هذا الاسلوب على عدة تقنيات منها كمثال على تقنيات شائعة في هذا المجال :

أ– حصان طروادة :(Trojan Horse)

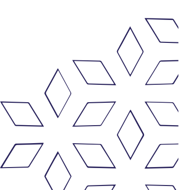
وهو برنامج يظهر بأنه يعمل بشكل معين ومفيد للمستخدم بينما هو في الواقع يقوم بعمل ضار وخفي عن المستخدم مثل الإضرار بالحاسوب أو إرسال معلومات إلى المحتال .

ب– الفيروسات :(Viruses)

وهي برامج تدخل إلى الحاسوب ويتصل بالملفات المخزنة به ثم يكرر نفسه بحيث يتم تدمير هذه الملفات .

ج– برامج التجسس :(Spyware)

وهي البرمجيات التي تؤدى إلى التجسس على المعلومات الشخصية دون علم مستخدم الحاسوب وغالبا ما يتم تنزيلها بشكل سري بحيث تكون مرافقة لتنزيل برمجيات أو ملفات مجانية من الإنترنت.



❖ العلاقة بين مستويات أمان المعلومات

نظرا لصعوبة تحقيق الأمن اتجهت الدول إلى إقامة علاقات ذات طابع إقليمي ودولي تزيد من صلابة سياساتها الأمنية الوطنية، **وصنفت تلك التكتلات في مستويات تتدرج من الفردية إلى الدولية كما يلي:**

المستوى الفردي: إن التركيز على الفرد كمستوى رئيسي في التحليل الأمني جاء من المخاوف المثار حول علاقة الفرد بالحكومة، حيث إن أمن الفرد لابد أن يكون في المقدمة دائما، **كما يركز على ٣ نقاط:**

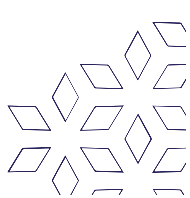
الدولة لا تقدم الأمن لكافة سكانها، بل على استعداد أن تتخلى على أمن أفرادها في سبيل كيانها، هناك دول تفشل في توفير الاحتياجات الضرورية لسكانها كالصومال، وأخرى تنتهك حقوق أفرادها، الدول التي تدعي أنها دولاً حارسة، فإنها قد تقوم بذلك بهدف الوصول إلى أمنها كدولة، ولا يتم التركيز على أمن الأفراد بشكل خاص، ويركز "بريان" جوب على أن أمن الأفراد والفئات الاجتماعية في دول العالم الثالث، حيث يرى أن الأمن لهؤلاء لم يتحسن بعد انتهاء الحرب الباردة إلى حد الان، يعيشون في اضطهاد وعليه فإن الأمن الفرد هو وصول الإنسان إلى حالة من الطمأنينة، وقدرته على ممارسة الخيارات المختلفة من خلال توفير سبل الحياة الاقتصادية الهانئة من خلال عمل ثابت ودخل ملائم.

المستوى الوطني : يركز على مجمل الأخطار الداخلية والخارجية التي تمس كيان الدولة **ويرى البعض أن أمن الدولة يشمل عنصرين:**

–حماية كيان الدولة ضد أعمال العدوان وسياسات التوسع، يستلزم قيام قوة عسكرية تمكنه من أداء هذه الوظيفة.

-حماية النسيج الداخلي للدولة وعدم تعرضها لحرب دعائية أو ضغوط اقتصادية أو عمليات إرهابية.

ويعرف الأمن الوطني على أنه: التعبير السياسي والاجتماعي عن الحالة الحقيقية التي يعيشها المجتمع وهو مفهوم ديناميكي يتفاعل ضمن دوائر ثلاث محلية، إقليمية، دولية، ويتضمن أمن المواطن ومستهلكاته وتاريخيه وتراثه ومعتقداته وحرياته الأساسية وسيادة الدولة.



المستوى الإقليمي :يرتبط بالنظام الإقليمي في منطقة **معينة ويشترط فيه:**

–يشمل ثلاث دول على الأقل.

–أن يتعلق بمنطقة جغرافية معينة.

–أن تكون ذات صفات ومميزات مشتركة تدفعها نحو التفاعل فيما بينها.

ويمكن تعريفه بأنه اتخاذ خطوات متدرجة تهدف إلى تنسيق السياسات الدفاعية بين أكثر من طرف وصولاً إلى تبني سياسة دفاعية موحدة تقوم على تقدير موحد لمصادر التهديد وسبل مواجهتها.

يرى البعض أنها سياسة مجموعة من الدول تنتمي إلى إقليم واحد تسعى إلى الدخول في تنظيم وتعاون عسكري لدول الإقليم لمنع أي قوة أجنبية من التدخل في هذا الإقليم **ومن نماذج التعاون في الأمن نذكر:**

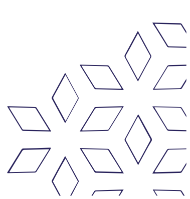
–الأنظمة الأمنية :أي تعاون مجموعة من الدول.

–المجتمع الأمني :مجموعة دول يوجد بينها تأكيد حقيقي لا يدخلون في حرب بينهم.

–الأحلاف :تلك المعاهدات تبرم بين دولتين أو أكثر.

–الكتلة الدولية :أي اتباع مجموعة من الدول نهج مشترك فيما بينهم.

الائتلاف وهو اتفاق بين مجموعة من الدول على تحقيق هدف أو مجموعة من الأهداف.

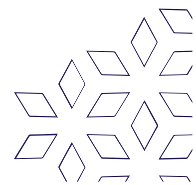


المستوى الدولي: المقصود بالنظام الدولي هي مجموعة من الأحداث السياسية المستقلة التي تتفاعل فيما بينها بانتظام، أو هي مجموعة من التحولات والتغيرات التي يشهدها العالم والتي مازالت في طور التكوين الكوني ولم تتبلور بعد في شكل كامل.

ويمكن اعتباره على أنه مجموعة من الوحدات السياسية المتدرجة لجهة القوة والمتفاعلة في علاقاته على نحو يهيئ لاتزان قواها ولانتظام علاقاتها بعيدا عن الفوضى.

أعطت الأمم المتحدة تصوراً للأمن الدولي يشمل عدة آليات:

يتعين على الدول الالتزام بمجموعة من المبادئ والوقائع منها: عدم التدخل في الشؤون الداخلية للدول الأعضاء، عدم اللجوء لاستخدام القوة والتهديد، وتسوية النزاعات بالطرق الدبلوماسية، وجود هيئة مسؤولة عن مراقبة سلوك الدول والحفاظ على السلم والأمن الدولي، وجود مجموعة من الأجهزة والآليات المساعدة التي تهدف إلى التعاون الدولي.

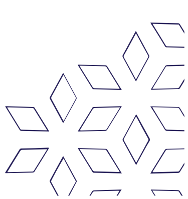


❖ الأمان وعلاقته بالتكلفة أو بالزمن

تخيل عالماً تقدم فيه شـركات الأمن السـيبراني تكاليف ثابتة لخدماتها، سـيكون تخطيط ميزانية تكنولوجيا المعلومات الخاصـة بك أسـهل، وسـتكون اتفاقيات الخدمة أبسـط، وسـيكون الأمن السيبراني في متناول الجميع، لسوء الحظ، هذا بعيد كل البعد عن الواقع.

هناك الكثير من الأشـياء التي يجب مراعاتها عندما يتعلق الأمر بالأمن السـيبراني، تلعب عوامل مثل الصناعة التي تعمل فيها في مجال انتشار التهديدات الإلكترونية الجديدة دورها، هذا هو السبب في أنه من الضـروري اختيار الحلول الأمنية التي تناسـب احتياجاتك، وإلا، فقد تدفع الكثير مقابل شـيء لا تحتاجه، أو أسوأ من ذلك، قد تدفع القليل جداً لحماية شبكتك بشكل صحيح.

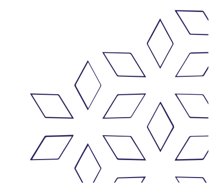
ومن الأهمية بمكان لاي حكومة او شـركة او منظمة معرفة حجم ما هو ضـروري للاسـتثمار في الأمن السيبراني والى أي مدى هو كاف من خلال تحليل استراتيجيات الأمن السيبراني على المستوى الوطني (NCSS) national cyber security strategies ، وذلك للعمل على تقييم العناصـر الاقتصـادية الأساسية لصياغة واعتماد نموذج من استراتيجيات الأمن السيبراني على المستوى الاقليمي،ومعالجة ذلك من منظور صـنع السـياسـات العامة للدولة ،ومحاولة قياس تكلفة انعدام الأمن السـيبراني ، وتقييم الكفاءة والحوافز الاقتصـادية لجميع أصـحاب المصـلحة المعنيين، وبذلك فقد عدت قضـية الامن السيبراني وعلاقته بالاقتصاد من ضمن الأهداف بالغة الاهمية لكافة اصحاب المصلحة، وذلك من اجل تحقيق الرخاء الاقتصادي للمجتمعات البشرية.



تتطور الجرائم الإلكترونية، وكذلك أدواتها وتكتيكاتها وإجراءاتها، تستفيد مجموعات المجرمين الإلكترونيين المحترفين والجهات الفاعلة في الدولة القومية ومجموعات التهديدات المستمرة المتقدمة (APT) أيضًا من ثغرات يوم الصفر – وهي الهجمات التي تركز على استغلال الثغرات الأمنية التي لم يتم تصحيحها من قبل بائعي البرامج حتى الآن لأنه ليس لديهم معلومات عنها في ذلك الوقت أو لأنهم يحتاجون إلى مزيد من الوقت لتطوير التصحيح وتوزيعه بشكل صحيح على جميع عملائهم، في حالة المنتجات الشائعة التي تستخدمها المؤسسات على نطاق واسع ، قد يؤدي مثل هذا الموقف إلى إنشاء نافذة كبيرة للتعرض ، مما يجعلها غير محمية تماماً في هذا الإطار الزمني.

يحتاج المهاجمون إلى ثوانٍ فقط لاستغلال الثغرة الأمنية، في حين أن الصناعة بأكملها قد تنتظر أياماً (في بعض الحالات أشهر) حتى يتم إصدار التصحيح، حدثت مثل هذه المواقف في شتاء عام ٢٠١٩ عندما كان المهاجمون يقومون بمسح كبير للإنترنت بحثاً عن مضيفي الشبكة باستخدام منتجات VPN معينة بها ثغرة أمنية خطيرة لتنفيذ التعليمات البرمجية عن بُعد (RCE). في غضون دقائق، تم اختراق آلاف الشركات، استغرق الأمر أسابيع حتى يقوم البائع بإصدار تصحيح بعد اكتشاف أنشطة ضارة تستهدف منتجهم على مستوى العالم، تكرر نفس الموقف مرة أخرى هذا العام في وقت عيد الميلاد، عندما كان المدافعون وشركات التكنولوجيا أقل استباقية.

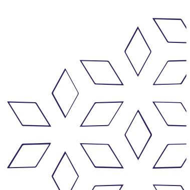
في الأمن السيبراني، تحدد السرعة نجاح كل من المدافع والمهاجم، يستغرق مجرم الإنترنت المستقل حوالي ٩,٥ ساعات للوصول غير المشروع إلى شبكة الهدف، كل دقيقة لا تستخدمها الشركة لصالحها تمنح المتسللين فرصة لإحداث ضرر أكبر.



قد يستغرق الأمر أيام عمل، إن لم يكن أسابيع، لتحديد الانحرافات الأمنية أو نشاط الشبكة المشبوه أو محاولات القرصنة، تقضي الشركة في المتوسط ١٩٧ يوماً لتحديد الخرق الأمني و ٦٩ يوماً لاحتواء الخرق الأمني، لايمكن لأي نقاش حول أهمية السرعة في الأمن السيبراني استبعاد مؤشرات الأداء الرئيسية لـ DevOps مثل MTTD و MTTF و MTBF و MTTR.

تشكل MTTD وMTTF وMTBF و MTTR مفهوم السرعة في الأمن السيبراني، يؤدي تنفيذ مؤشرات الأداء الرئيسية المستندة إلى الوقت إلى تحويل تركيز استراتيجية المدافع من رد الفعل إلى الاستباقي.

- MTTD (متوسط الوقت اللازم للكشف) هو مقدار الوقت الذي تستغرقه الشركة لتحديد حادثة أمنية محتملة.
- MTTF(متوسط الوقت حتى الفشل) هو المدة التي يمكن أن يعمل بها النظام المعيب حتى يتم إيقاف تشغيله.
- MTTR (متوسط وقت الاستجابة) هو الوقت الذي يستغرقه الفريق للسيطرة على التهديد أو علاجه أو القضاء عليه بعد تحديده.
- MTBF (متوسط الوقت بين الإخفاقات) يعكس موثوقية وتوافر النظام، يتم استخدامه لتقييم أداء النظام في ظل ظروف محددة مسبقاً لفترة زمنية محددة.

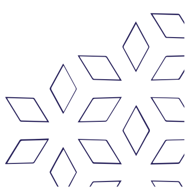


❖ التخطيط الاستيراتيجي للأمن السيبراني

يوجد أمن المعلومات لمساعدة قادة الأعمال على فهم وإدارة مخاطر التكنولوجيا المعقدة، يقع على عاتق قادة الأعمال التزام ائتماني بحماية البيانات من الفقد أو الكشف أو التغيير غير المصرح به ، ويجب عليهم التأكد من أن أنظمتهم متاحة عند الحاجة – خاصة في أوقات الأزمات، في مواجهة هجمة الانتهاكات الكارثية ، يسعى قادة الأعمال إلى مواجهة ضغوط الامتثال الجديدة حيث يستجيب المنظمون بمزيد من التفويضات، في هذا العالم المعقد والعدائي بشكل متزايد ، يحتاج قادة الأعمال إلى مستشار موثوق به لمساعدتهم على النجاح وحماية سمعتهم، أمن المعلومات يملأ هذا الدور.

يواجه أمن المعلومات تحديات غير مسبوقة وفرصاً غير عادية، أصبحت الهجمات المتقدمة أكثر تعقيداً وأكثر شيوعاً ، حيث تختبر حدود القدرات الحالية، دفع الشركات إلى الرقمنة يضاعف المشكلة ويوسع بشكل كبير حجم البيانات التنظيمية الحساسة المعرضة للهجوم، تضع هذه الاتجاهات وغيرها ضغطاً كبيراً على مسؤولي أمن المعلومات في القطاعين العام والخاص لتطوير استراتيجيات وتكتيكات جديدة للنجاح.

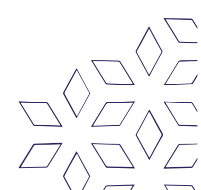
يعتقد أكثر من نصف CISOs في الولايات المتحدة أن هجوماً متقدماً سيؤثر على منظمتهم في العام المقبل، إن انتشار هذه التهديدات يعني أنه يجب على CISOs تطوير كفاءات استخبارات التهديدات المتطورة بسرعة مع تحسين خطط الاستجابة عندما يحدث الأسوأ، يستخدم المهاجمون كل يوم أدوات وأساليب متطورة لاختبار دفاعات ولاية مينيسوتا والكيانات الحكومية الأخرى، لسوء الحظ، فإن العديد من الهيئات الحكومية لاترقى إلى مستوى التحدي، والنتيجة هي انتهاكات مكلفة ومحرجة للبيانات تقوض ثقة المواطنين في الحكومة وتكلف دولارات كبيرة.



تشهد كل من المنظمات الحكومية والقطاع الخاص زيادات كبيرة في خسائر الأمن السيبراني بسبب الانتهاكات والتخفيضات في إنتاجية العمال، لدى المنظمات في الولايات المتحدة الآن متوسط خسائر سنوية في الجرائم الإلكترونية يبلغ ١٥,٤ مليون دولار ، وفقاً لدراسة تكلفة جرائم الكمبيوتر لعام ٢٠١٥ الصادرة عن معهد بونيمون، زيادة بنسبة ١٩ في المائة عن عام ٢٠١٤ ، وهذا يمثل ضعف متوسط معدل الخسارة في الدول الصناعية الأخرى، تُظهر النتيجة الرئيسية في التقرير أن نشر تقنيات الأمان المتقدمة يحدث فرقًا كبيراً لتقليل خسائر الأمن السيبراني بشكل كبير.

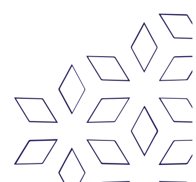
أدى التركيز المكثف العام والإعلامي والتنظيمي على الهجمات الإلكترونية إلى زيادة اهتمام كبار المسؤولين التنفيذيين بأمن المعلومات، ولهذا السبب ، حددت الرابطة الوطنية لكبار مسؤولي المعلومات في الدولة (NASCIO) أمن المعلومات كأولوية رقم واحد لمدة عامين متتاليين، كما قادت NASCIO ثلاث دراسات على مدى السنوات الأربع الماضية مع شركة استشارية رائدة لتسليط الضوء على قضايا التمويل والحوكمة التي تمنع فعالية برامج أمن الدولة، لقد أصبح أمن المعلومات قضية مهمة على مستوى قيادة الولاية ، وقد ظهر في يوليو عندما وقع ٣٨ حاكماً ، بمن فيهم حاكم مينيسوتا مارك دايتون ، اتفاقاً يتعهدون فيه بالتزامهم بتعزيز دفاعات الأمن السيبراني في ولاياتهم.

من المهم ملاحظة أن حكومات الولايات في المتوسط تنفق حوالي ٢٪ من ميزانيتها الخاصة بتكنولوجيا المعلومات على الأمن السيبراني، مقابل ٥٪ أو أكثر ينفقها القطاع الخاص والوكالات المدنية الحكومية الفيدرالية، في حين كان الإنفاق الحكومي ثابتاً، أعلنت شركة جارتنر مؤخراً أن الإنفاق العالمي على الأمن السيبراني يتزايد بمعدل سبعة إلى تسعة بالمائة.



من الواضح أن المؤسسات في جميع أنحاء العالم تعمل على رفع مستوى الأمن السيبراني استجابةً للتهديدات الأكثر تقدماً واستمراراً، تقوم المنظمات التي لاتواكب العمل بتراكم ديون متعلقة بالأمن السيبراني يتعين عليها في النهاية دفعها لتتماشى مع أفضل الممارسات المقبولة في الصناعة.

على الرغم من أن الخطة الإستراتيجية لأمن المعلومات لا تدعو على وجه التحديد إلى مزيد من الإنفاق لجعل الأمن "أكبر"، إلا أنها تحدد الخطوات التي يجب اتخاذها لجعل الأمن "أفضل" تعطي هذه الخطة الأولوية لمبادرات إدارة ومراقبة وحماية أصول معلومات الدولة، ويحدد ١٨ استراتيجية رئيسية تأمل Minnesota IT Services (MNIT) في تحقيقها على مدى السنوات الخمس المقبلة، إذا سمحت الموارد بذلك، كما تسلط الخطة الضوء على معالم محددة للسنة التالية ، وهي الأشياء التي تتوقع MNIT تحقيقها بالموارد الموجودة.

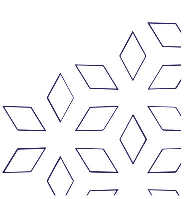


تنظم الخطة الاستراتيجيات والمعالم في أربعة محاور:

١- إدارة استباقية للمخاطر:

تعمل بعض أهم استراتيجيات الأمان على منع حدوث أحداث أمنية معاكسة، مع التهديدات الأكثر تقدماً واستمراراً، عادةً ما تقوم المؤسسات الكبيرة بتشغيل أدوات متطورة للمساعدة في إدارة المخاطر الإلكترونية في الوقت الفعلي. ومن الأمثلة على إحدى هذه الأدوات برنامج إدارة الثغرات الأمنية، والذي يساعد المتخصصين في مجال الأمن في العثور على الثغرات الأمنية وإصلاحها قبل أن يستغلها المتسللون، تتضمن إدارة المخاطر الاستباقية أيضاً فهم الخصوم وتصميم حلول لمكافحة نواقل التهديد المعروفة، مثل هجمات رفض الخدمة، أخيراً، يعد تعليم الموظفين دفاعاً وقائياً مهماً في عالم يتزايد فيه العداء، حيث غالباً ما يكون الأشخاص هدفاً يختاره المخترقون.

توفر هذه الخطة أيضاً لقادة الأعمال فهماً أفضل بكثير لمخاطر الأمن السيبراني، ستقدم MNIT بطاقات أداء المخاطر الإلكترونية لقيادة الوكالات الشريكة لنا، وتزويدهم بمقاييس مستمرة لفهم وإدارة وضعهم من المخاطر، ستشرك MNIT أيضاً قادة الأعمال في محادثات المخاطر الإلكترونية خلال مشاريع تطوير النظام الرئيسية.



٢- تحسين الوعي بالظروف:

الوعي بالظروف هو مفتاح برنامج أمان فعال، يسمح الوعي بالتهديدات، سواء الكوارث الطبيعية أو ذات الدوافع البشرية، بالتخصيص الفعال للموارد والتنفيذ الفعال للضوابط، يساعد الوعي بنقاط الضعف في تحديد أولويات جهود الإصلاح، والوعي بالأحداث الأمنية يؤدي إلى اتخاذ إجراءات استجابة مناسبة وفي الوقت المناسب.

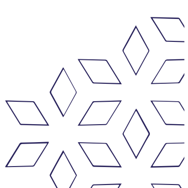
ستساعد الاستراتيجيات في هذه الفئة الدولة على فهم مخاطرها وتهديداتها بشكل أفضل والاستجابة السريعة للأحداث السلبية، كما أنها تمنح الدولة مقياساً أكثر فاعلية لموقفها من المخاطر بمقاييس أداء صارمة.

– <u>كشف الأخطاء الأمنية بشكل أسرع:</u>

تتضمن العمليات الأمنية الأنشطة اليومية للمراقبة والتدقيق والاستجابة للأحداث ربط كميات هائلة من المعلومات والتعاون مع العديد من الفرق، لكي تؤدي حكومة الولاية هذه العمليات بشكل جيد، يجب أن تكون البيانات متاحة ودقيقة، ويجب ضبط الأدوات وتكاملها، ويجب اختبار العمليات وتنضجها باستمرار، إن الزيادة المستمرة في تعقيد تكنولوجيا المعلومات بالولاية وتشغيل أنظمة الحالة على مدار ٢٤ ساعة يزيد من الحاجة إلى عمليات أمنية أكثر فعالية.

- <u>تحسين فهمنا لبيئة تكنولوجيا المعلومات:</u>

هناك قول مأثور قديم في مجال الأمن السيبراني، لايمكنك تأمين ما لا تفهمه، يعد تحديد ضوابط الأمان في عالم من التهديدات سريعة التغير أمراً صعباً، لاسيما في البيئات شديدة التعقيد والمتنوعة للغاية، ستساعد هذه الاستراتيجية برنامج أمن الدولة على اكتساب فهم أكثر شمولاً لأنظمة الأعمال التي يدعمها الآن، بما في ذلك الأجهزة والبرامج التي يقوم عليها كل نظام.



٣- الأزمة القوية والاستجابة للحوادث

ليس من الممكن منع كل حادث أمني يمكن تصـوره يمكن أن يؤثر على أنظمة معلومات الدولة، يتضمن برنامج أمن المعلومات المتوازن القدرة على تحليل الظروف المحيطة بالحادث واستعادة وظائف النظام العادية في الوقت المناسب.

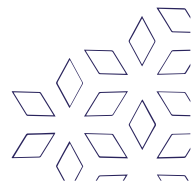
يجب أن يكون لدى MNIT خطط قوية لتقليل تأثير الحوادث الأمنية، يجب على MNIT أيضاً اختبار تلك الخطط وعمليات الاسـترداد للحفاظ على عمل الخدمات الحيوية وتأمين البيانات في وقت الأزمات.

- **<u>تطوير وممارسة استراتيجيات الاسترداد للتطبيقات:</u>**

توثق خطة التعافي من الكوارث اسـتراتيجيات التعافي لنظام المعلومات. وهي تحدد إجراءات الاسـتجابة والتعافي المحددة سـلفاً والمعتمدة التي تقلل من اتخاذ القرار أثناء الأزمة، وتوفر عملية انتعاش منهجية وموثقة، تضـمن إجراءات التعافي من الكوارث المخطط لها استعادة وظائف الأعمال الحيوية في الوقت المناسب في أوقات الأزمات

- **<u>الاستجابة للحوادث الأمنية بشكل أسرع:</u>**

تؤدي العمليات الرسـمية لتسـجيل الحوادث الأمنية والتحقق منها وترتيب أولوياتها وتصنيفها واحتوائها والقضاء عليها إلى تقليل الضرر الناتج عن الهجمات. يمكن للعلاقات القوية والتواصل المستمر أن يساعد أيضاً المتخصصين في مجال الأمن على الاستجابة للحوادث بشكل أسرع، يعد تبسيط عمليات الاستجابة جزءاً أساسياً من هذه الاستراتيجية، يؤدي التطبيع الإضـافي لعمليات الاسـتجابة القديمة إلى تقليل الوقت الذي يسـتغرقه التحقق من الحوادث والاستجابة لها، لا سيما في حالة الحوادث التي تحدث خلال ساعات غير العمل.



٤- شريك للنجاح

مع ظهور الأنظمة المترابطة والإنترنت، تعمل حكومة الولاية في عالم معادي للغاية، تأتي هجمات القراصنة ضد حكومة الولاية من كل دولة، ولا تتوقف أبداً، في كل يوم، يحاول الأفراد عديمو الضمير اختراق أنظمة الدولة لسرقة البيانات وإغلاق الخدمات الحيوية واستخدام البنية التحتية للتكنولوجيا لدينا لشن هجمات مجهولة ضد الآخرين.

تتطور أساليب هجوم القراصنة يومياً، مما يجبر المتخصصين في مجال الأمن على تعديل دفاعاتهم في معركة متواصلة تنطوي على مخاطر عالية جداً، يعتمد النجاح على معلومات التهديد، عند حدوث هجمات معقدة، يمكن أن يعني الإنذار المبكر ونصائح الخبراء الفرق بين استمرارية الأعمال والكارثة، لقد تطور الأمن السيبراني الآن إلى نظام بيئي يتوقف فيه نجاح كل مؤسسة على استخبارات التهديدات في الوقت المناسب والقابلة للتنفيذ.

من خلال استخدام استخبارات الصناعة، وتدريب خبراء الإنترنت في المستقبل، والعمل مع الاستجابة للطوارئ، ستبني MNIT العلاقات اللازمة لمكافحة الجرائم الإلكترونية الآن وفي المستقبل.

- <u>**استخدم الشراكات الإستراتيجية لتحسين الأمان:**</u>

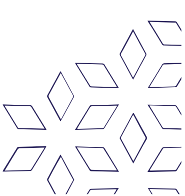
  تتضمن هذه الإستراتيجية المشاركة في النظام البيئي المحلي والوطني لذكاء التهديدات، ويشمل أيضاً توسيع النظام البيئي لذكاء التهديدات للدولة، ودمج منتجات استخبارات التهديدات التجارية في السوق الآن.

- <u>**تطوير برنامج تغذية المواهب مع التعليم العالي:**</u>

  تسمح الشراكة المستمرة مع المؤسسات التي لديها برامج إلكترونية لشركة MNIT بإظهار فوائد العمل في الدولة، مع التأكيد أيضاً على أن الطلاب لديهم المهارات التي يحتاجون إليها للحصول على وظائف ناجحة في مجال تكنولوجيا المعلومات

- <u>**توفير حضور إلكتروني في مركز الانصهار الحكومي:**</u>

  تجمع مراكز الاندماج بين منظمات الاستجابة لتبادل المعلومات الاستخباراتية لحماية المجتمعات المحلية، تم توجيه مراكز الاندماج تاريخياً نحو التهديدات المادية، لكن قادة مراكز الاندماج يدركون أن الجهات الفاعلة في مجال تهديد الأمن السيبراني تشكل أيضاً خطراً كبيراً على المجتمع.



❖ التصديق الرقمي

حتى تكتمل عملية التحول الرقمي لابد من الاهتمام بالتوثيق الإلكتروني باستخدام الشهادة الرقمية والتوقيع الرقمي وإصدار هذه الشهادات من الوزارات والهيئات الحكومية ووضع الأنظمة والقوانين والتحول إلى اعتماد شهادات التصديق الإلكتروني في إجراء المعاملات الحكومية ومعاملات القطاع الخاص، وقد أسست المملكة المركز الوطني للتصديق الإلكتروني لإصدار الشهادة الرقمية في عام ٢٠٠١.

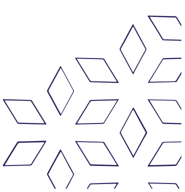
شهادة التصديق الرقمي: هو وثيقة إلكترونية يصدرها مقدم خدمات تصديق، تستخدم لتأكيد هوية الشخص الحائز على منظومة التوقيع الإلكتروني، وتحتوي على بيانات التحقق من توقيعه، ويصاحب كل شهادة رقمية مصدّرة عادة مفتاح عام ومفتاح خاص يستخدم أحدهما للتشفير أو التوقيع الإلكتروني والآخر لفك التشفير أو التحقق من التوقيع الإلكتروني.

أما التوقيع الرقمي فهو عبارة عن شهادة على شكل ملف رقمي يحتوي على الاسم يصدر عن إحدى الهيئات المتخصصة بهذا الموضوع ومعترف بها وهي تحتوي توقيعك الإلكتروني الذي يميزك عن بقية الناس.

والفرق بين التوقيع الرقمي وشهادة التصديق الرقمي:

– في التوقيع الرقمي لا يوجد ضمان أن المفتاح العام هو لهذا الشخص بالفعل أي أنه في التوقيع الرقمي لا يوجد ربط بين الشخص بالفعل ومفتاحه العام (الفتاح العام موجود على الشهادة الموجودة على المخزن العام).

– الشهادة الرقمية والتي تربط بين الشخص ومفتاحه العام والمفتاح الخاص حيث تحتوي الشهادة على صاحب الشهادة ومفتاحه العام وموقعة من طرف موثوق فيه يثبت ذلك.

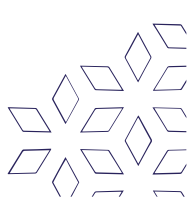


وهناك أنواع من الشهادة الرقمية مثل:

- الشهادات المخصصة لأغراض التشفير.
- الشهادات المخصصة لأغراض التحقق من الهوية الإلكترونية.
- الشهادات المخصصة للتوقيع الرقمي والتي تعرف بأنها الهوية الإلكترونية للشخص.

وتوضع أسس للحصول على الشهادة الرقمية من قبل الجهة المرخصة لإصدار مثل هذه الشهادات، ويجب أن تشمل شهادة التوثيق الإلكتروني التي تصدرها جهة التوثيق الإلكتروني **بحيث تتوافق على العناصر التالية:**

- الغرض من استخدام الشهادة.
- موضوع الترخيص أو الاعتماد لجهة التوثيق المرخصة والمعتمدة، يوضح فيها نطاقه ورقمه وتاريخ إصداره وفترة سريانه.
- اسم جهة التوثيق المصدرة للشهادة والدولة التابعة لها.
- الجهة التي تم إصدار الشهادة لها.
- المفتاح العام.
- تاريخ صلاحية الشهادة وتاريخ انتهائها.
- الرقم المتسلسل للشهادة ورقم الإصدار.
- التوقيع الإلكتروني لجهة التوثيق الإلكتروني التي أصدرت الشهادة والخوارزمية المستخدمة.
- عنوان الموقع الإلكتروني المخصص لقائمة الشهادات الملغاة أو الموقوفة.
- خوارزمية بصمة الإبهام(Thumbprint Algorithm)
- بصمة الإبهام(Thumbprint) .



❖ أنظمة كشف التطفل IDS

نظام كشف التسلل (IDS) هو برنامج مصمم خصيصاً لمراقبة حركة مرور الشبكة واكتشاف المخالفات، حيث تشير تغييرات الشبكة غير المبررة أو غير المبررة إلى نشاط ضار في أي مرحلة، سواء كان ذلك بداية هجوم أو اختراق كامل، هناك نوعان رئيسيان من أنظمة كشف التسلل (IDS) هما، نظام كشف التسلل عبر الشبكة (NIDS) ونظام كشف التسلل المعتمد على المضيف (HIDS) .

"IDS"هي اختصار لـ"Intrusion detection system"

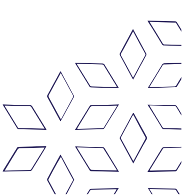
"HIDS"هي اختصار لـ"Host-based intrusion detection system"

كيف يعمل نظام كشف التسلل؟

بعد جمع البيانات، يتم تصميم نظام كشف البيانات (IDS) لمراقبة حركة مرور الشبكة ومطابقة أنماط حركة المرور بالهجمات المعروفة، ومن خلال هذه الطريقة التي تسمى أحياناً ارتباط النمط، يمكن لنظام منع التطفل تحديد ما إذا كان النشاط غير العادي هو هجوم إلكتروني، وبمجرد اكتشاف نشاط مشبوه أو ضار، سيرسل نظام كشف التسلل إنذاراً إلى الفنيين أو مسؤولي تكنولوجيا المعلومات المحددين، حيث تمكّن إنذارات (IDS) من البدء بسرعة في استكشاف الأخطاء وإصلاحها وتحديد المصادر الجذرية للمشكلات، أو اكتشاف العوامل الضارة وإيقافها في مساراتها.

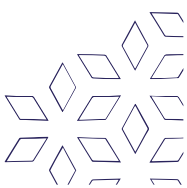
طرق كشف التسلل تستخدم أنظمة كشف التسلل في المقام الأول طريقتين رئيسيتين لكشف التسلل، وهما كشف التسلل المستند إلى التوقيع واكتشاف التسلل المستند إلى الشذوذ، ويتم تصميم كشف التسلل المستند إلى التوقيع لاكتشاف التهديدات المحتملة من خلال مقارنة حركة مرور الشبكة وبيانات السجل بأنماط الهجوم الحالية، كما تسمى هذه الأنماط التسلسلات، ويمكن أن تتضمن تسلسلات البايت، والمعروفة باسم تسلسل التعليمات الضارة، يمكّن الاكتشاف المستند إلى التوقيع من الكشف الدقيق عن الهجمات المعروفة المحتملة والتعرف عليها، إن اكتشاف التسلل المستند إلى الشذوذ هو عكس ذلك، فهو مصمم لتحديد الهجمات غير المعروفة، مثل البرامج المؤذية الجديدة، والتكيف معها بسرعة باستخدام التعلم الآلي، كما تتيح تقنيات التعلم الآلي لنظام اكتشاف التطفل (IDS) إنشاء خطوط أساسية للنشاط الجدير بالثقة المعروف باسم نموذج الثقة، ومن ثم مقارنة السلوك الجديد بنماذج الثقة التي تم التحقق منها، يمكن أن تحدث الإنذارات الكاذبة عند استخدام (IDS) المستند إلى الانحراف، حيث يمكن تحديد حركة مرور الشبكة غير المعروفة سابقاً ولكنها مشروعة على أنها نشاط ضار.

حيث تستخدم أنظمة الكشف عن التسلل الهجين كشف التسلل المستند إلى التوقيع والقائم على الانحراف لزيادة نطاق نظام منع التطفل، يمكّن هذا من تحديد أكبر عدد ممكن من التهديدات، ويمكن لنظام كشف التسلل الشامل (IDS) فهم تقنيات التهرب التي يستخدمها مجرمو الإنترنت لخداع نظام منع التطفل للاعتقاد بعدم وقوع هجوم، يمكن أن تشمل هذه الأساليب التجزئة وهجمات النطاق الترددي المنخفض والتهرب من تغيير النمط وانتحال العناوين أو الوكلاء، وأكثر من ذلك.



لماذا يعد استخدام نظام كشف التسلل مهماً؟

- يمكّن لنظام (IDS) من تعزيز أمان أجهزة الشبكة وبيانات الشبكة القيمة عن طريق تحديد حركة مرور الشبكة المشبوهة ولفت الانتباه إليها، كما تحتاج الشبكة إلى أمان قوي لحماية المعلومات الحالية وعمليات نقل بيانات الشبكة الداخلية والخارجية، تتزايد الهجمات الإلكترونية من حيث التعقيد والانتظام، لذا من المهم أن يكون لديك نظام اكتشاف اقتحام شامل وقابل للتكيف، إلى جانب زيادة أمان الشبكة، يمكن أن يساعدك نظام كشف التسلل في تنظيم بيانات الشبكة الهامة.
- تنشئ الشبكة الكثير من المعلومات كل يوم من خلال عمليات منتظمة، حيث يساعد نظام كشف التسلل في التمييز بين النشاط الضروري والمعلومات الأقل أهمية، وذلك من خلال المساعدة في تحديد البيانات التي يجب الانتباه إليها.
- يمكن لنظام الكشف عن التسلل أن يمنع المستخدم من التمشيط عبر آلاف سجلات النظام للحصول على معلومات مهمة، كما يمكن أن يوفر ذلك الوقت ويقلل الجهد اليدوي ويقلل من الخطأ البشري عندما يتعلق الأمر باكتشاف التسلل، يمكن ان يساعد في الحصول على رؤية مفصلة ودقيقة لنشاط الشبكة من خلال (IDS) في إظهار الامتثال، حيث تم تصميم أنظمة منع التطفل لاكتشاف وتنظيم وتنبيه حركة مرور الشبكة الواردة والصادرة، وتحديد المعلومات الأكثر أهمية، وذلك من خلال التصفية من خلال حركة مرور الشبكة، كما يمكن أن يمنح نظام الكشف عن التطفل خطوة عندما يتعلق الأمر بتحديد مدى امتثال الشبكة وأجهزتها، حيث تم تصميم (IDS) لتحسين اكتشاف التسلل والوقاية منه عن طريق التصفية من خلال تدفق حركة المرور، ويمكن أن يوفر هذا الوقت والطاقة والموارد أثناء اكتشاف النشاط المشبوه قبل أن يتحول إلى تهديد كامل.
- يوفر (IDS) أيضاً رؤية متزايدة لحركة مرور الشبكة، والتي يمكن أن تساعد على صد النشاط الضار واكتشافه، وتحديد حالة التوافق، وتحسين الأداء العام للشبكة، حيث انه كلما اكتشف نظام (IDS) الخاص النشاط الضار على الشبكة، زادت قدرته على التكيف مع الهجمات المعقدة بشكل متزايد.



ثالثاً: سياسات الأمن السيبراني ومعاييره

في هذا الفصل سنتعرف على المواضيع التالية:

- مفهوم السياسة الأمنية وأهميتها
- أنواع السياسات الأمنية
- مفهوم المعايير القياسية وتصنيفها واستخدامها
- اللوائح والقوانين المتعلقة بالأمن السيبراني
- الأطراف المعنية بتنفيذ القواعد التي يجب الالتزام بها
- المعايير العالمية للأمن السيبراني
- تصنيف المعلومات ومستوياتها
- التدريب والتوعية بالأمن السيبراني

❖ مفهوم السياسة الأمنية وأهميتها

يحتاج الإنسان إلى الشعور بالأمان في جميع أحواله، ويمكن تقسيم الأمن اعتماداً على المنطقة الجغرافية إلى: الأمن القومي والأمن الإقليمي والأمن الدولي، واعتماداً على الموضوعيّة يُقسم إلى: الأمن العام، والأمن السياسي، والأمن الاقتصادي، والأمن الاجتماعي، والأمن الجنائي، وأمن المنشآت، وأمن المعلومات وغيرها، يُعدّ الأمن السياسي امتداداً لمنظومة الأمن القومي في المجتمع، كالأمن الغذائي، والأمن المائي، والأمن القومي، فكلّها تؤدي إلى استقرار المجتمع وزيادة قدرته على تقديم الخدمات لأفراده، وتحسين مستويات معيشتهم.

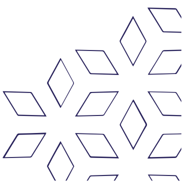
مفهوم السياسة الأمنية

الأمن في اللغة: الأمن من آمن يأمن أمناً فهو آمن، وأمِن بمعنى اطمأن ولم يخف فهو آمنٌ، والأمن هو الاستقرار والاطمئنان.

تعريف السياسة الأمنية: يمكن تعريف الأمن السياسي بأنه التحرر من الخوف والحاجة، وضمان تأمين الحماية من تهديد القمع السياسي، والحماية من التعرض للصراعات والحروب والهجرة لجميع المواطنين في الوقت ذاته دون استثناء أو تمييز على اعتبارها حقاً من الحقوق المكتسبة للإنسان، مما يقود إلى الاستقرار التنظيمي للدول، ونظم الحكومات والأيديولوجيات التي تستمد منها شرعيتها.

أهمية السياسة الأمنية

بناء المجتمع وتطويره، فالأمن السياسي يقود إلى حرية الأفراد في تقديم الأفكار والمساعدات المختلفة لتطوير مجتمعهم وتقدّمه بين مجتمعات العالم، زيادة الدخل الاقتصاديّ للدولة من خلال المشاريع التي يتم إنشاؤها، فالمستثمرون من جميع أنحاء العالم يبحثون عن المكان المستقر ليستطيعوا بناء مشاريعهم وتحقيق الأرباح منها، لذلك عندما يكون المجتمع آمناً سياسياً فإنه يجذب أصحاب رؤوس الأموال، المحافظة على مقتنيات المجتمع والأفراد، لأن الافتقار إلى الأمن السياسي يقود إلى نشوب الحروب والثورات والخلافات بين أبناء الطوائف السياسية المختلفة من الأفراد نتيجة انتماءاتهم السياسية، مما يقود إلى تكسير وتدمير الممتلكات العامة.



❖ أنواع السياسات الأمنية

- **السياسات الأمنية العامة**

مفهوم السياسة الأمنية العامة

هي قواعد عملية وفنية موثقة لحماية جهة ما من مخاطر أمن المعلومات التي تحدق بأعمالها وبنيتها التحتيةً التقنية، وتقدم وثائق السياسات هذه وصفاً عاماً للضوابط المختلفة التي ستستخدمها المؤسسة لإدارة مخاطر أمن المعلومات لديها، وتعتبر وثائق سياسات أمن المعلومات إعلاناً رسمياً عن نية الإدارة لحماية أصول المعلومات لديها من المخاطر ذات العلاقة.

قد تكون سياسات أمن المعلومات مدعومة بإجراءات لأمن المعلومات في بعض الحالات، وتبين هذه الإجراءات الأنشطة الرئيسية اللازمة لتطبيق تلك السياسات.

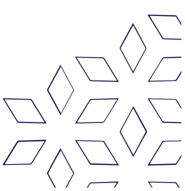
قامت الهيئة الوطنية للأمن السيبراني بتطوير الضوابط ألاساسية للأمن السيبراني لوضع الحد الأدنى من متطلبات الأمن السيبراني في الجهات الوطنية التي تندرج تحت نطاق عمل هذه الضوابط، وعلى مختلف الجهات الوطنية تنفيذ ما يحقق الالتزام الدائم والمستمر بهذه الضوابط، تحقيقاً لما ورد في الفقرة الثالثة من المادة العاشرة في تنظيم الهيئة الوطنية لأمن السيبراني وكذلك ما ورد في الأمر السامي الكريم رقم ٥٧٢٣١ وتاريخ ١٤٣٩/١١/١٠ هـ.

أمن الشركات

يشير أمن الشركات إلى مرونة الشركات ضد التجسس والسرقة والأضرار والتهديدات الأخرى، لقد أصبح أمن الشركات أكثر تعقيداً حيث ازداد الاعتماد على أنظمة تكنولوجيا المعلومات، وأصبح تواجدها الفعلي أكثر توزّعاً في العديد من البلدان بما في ذلك البيئات التي تُعتبر أو قد تصبح بسرعة معادية لها.

1. **أمن غذائي**

يشير الأمن الغذائي إلى الإمداد الجاهز للأغذية الآمنة والمغذية والحصول عليها، يكتسب الأمن الغذائي أهمية في الوقت الذي نما فيه سكان العالم وتضاءلت الأراضي المنتجة من خلال الاستخدام المفرط لها وتغير المناخ.



٢. أمن المنزل

عادةً ما يشير الأمن المنزلي إلى أنظمة الأمان المستخدمة في العقارات التي تستخدم كمسكن (بما في ذلك عادةً الأبواب والأقفال وأنظمة الإنذار والإضاءة والمبارزة)؛ والممارسات الأمنية الشخصية (مثل التأكد من أن الأبواب مقفلة، وأجهزة الإنذار، والنوافذ المغلقة).

٣. الأمن الإنساني

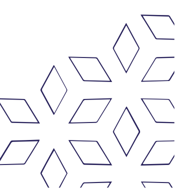
الأمن الإنساني هو اسم نموذج ناشئ رداً على التركيز التقليدي على حق الدول القومية في حماية نفسها، وركز على أولوية أمن الناس (الأفراد والمجتمعات)، تدعم الجمعية العامة للأمم المتحدة هذا المفهوم حيث شددت على «حق الناس في العيش في حرية وكرامة» وأقرّت بأن "جميع الأفراد،[٨] ولا سيما المستضعفين، لهم الحق في التحرر من الخوف والتحرر من العوز".

❖ مفهوم المعايير القياسية وتصنيفها واستخدامها

قامت الهيئة الوطنية للأمن السيبراني في المملكة بتطوير المعايير الأساسية للأمن السيبراني التي تهدف إلى توفير الحد الأدنى من المتطلبات الأساسية للأمن السيبراني المبنية على أفضل الممارسات والمعايير لتقليل المخاطر السيبرانية على الأصول المعلوماتية والتقنية للجهات من التهديدات الداخلية والخارجية، **تتكون الضوابط الأساسية للأمن السيبراني من ١١٤ ضابطاً أساسياً، مقسمة على خمس مكونات رئيسية، هي:**

- حوكمة الأمن السيبراني
- تعزيز الأمن السيبراني
- صمود الأمن السيبراني
- الأمن السيبراني المتعلق بالأطراف الخارجية والحوسبة السحابية
- الأمن السيبراني لأنظمة التحكم الصناعي

وتعتبر الضوابط الأساسية للأمن السيبراني ضوابط إلزامية، حيث يجب على جميع الجهات، ضمن نطاق عمل هذه الضوابط، تنفيذ ما يحقق الالتزام الدائم والمستمر بهذه الضوابط.



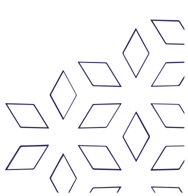
١. حوكمة الأمن السيبراني

تعريف حوكمة الأمن السيبراني: تُعرّف حوكمة الأمن السيبراني بالإنجليزية (Cybersecurity Governance) بأنّها النظام المكون من العمليات والإجراءات التي تُساعد المؤسسات على اكتشاف الهجمات السيبرانية، وتحديد كيفية الاستجابة لها، ومنع حدوثها، وتوضح حوكمة الأمن السيبراني بأنّه يجب أن يكون لكل جزء من النظام المسؤول عن مخاطر أمن المعلومات مالك، أو فريق يتحمل مسؤولية ضمان أهداف هذا الجزء، يجدر بالذكر بأنّ هناك فرق بين الحوكمة والإدارة، حيث تُركز الحوكمة على التخطيط الاستراتيجي، بينما تُركز الإدارة على الإشراف على تنفيذ أعمال الأمن السيبراني اليومية.

أهمية حوكمة الأمن السيبراني

تُساعد حوكمة الأمن السيبراني على حماية الشركات والمؤسسات من هجمات الجهات الخارجية، أو الجهات الداخلية التي تشمل الموظفين الحاليين والسابقين من خلال تركيزها على إدارة المخاطر، وزيادة الوعي في المؤسسات، وخاصةً المؤسسات ذات النظام المعقد، **بحيث تضمن حوكمة الأمن السيبراني للمؤسسة ما يأتي:**

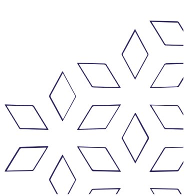
- التنسيق بين أهداف عمل المؤسسة واستراتيجيات تشغيل تكنولوجيا المعلومات، والتي توفر إجراءات تحسينية شاملة وحلول مدروسة تُمكن المؤسسة من الاستعداد لأي حوادث مُمكنة.
- بناء نظام رقابة فعّال.
- الدمج بين أنشطة إدارة المخاطر، وأنشطة الرقابة.
- تحسين الموارد الإنتاجية للمؤسسة.
- تبسيط الإجراءات المتعلقة بعمليات المراقبة والتدقيق.
- جمع البيانات الخاصة بالأعمال، وتقييمها بهدف تحسين جودتها، وضمان تحسينات مستقبلية أكثر أماناً.



تطبيق برنامج حوكمة الأمن السيبراني في المؤسسات

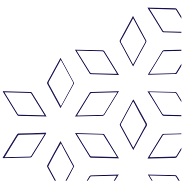
يجب على المؤسسات اتّباع ٦ خطوات أساسية لتطبيق برنامج حوكمة الأمن السيبراني، وهي كما يأتي:

- **دراسة الوضع الحالي:** يجب على المؤسسة فهم الثغرات الموجودة داخلها من خلال دراسة المخاطر الإلكترونية التي تواجهها وتقييمها، ثم التخطيط لإيجاد حلول لسد هذه الثغرات.
- **دراسة معايير وسياسات الأمن السيبراني:** يجب على المؤسسة دراسة جميع المعايير والسياسات والإجراءات الخاصة بالأمن السيبراني ومراجعتها وتحديثها باستمرار، ثم أخذ الوقت اللازم لتشكيل هيكل لحوكمة الأمن السيبراني داخل المؤسسة، وفقًا لهذه المعايير.
- **التعامل مع الأمن السيبراني من منظور المؤسسة:** يجب على المؤسسة تحديد أهم البيانات التي يجب حمايتها من أي هجمات خارجية، والنظر فيما إذا كانت إدارة المخاطر داخلها تتماشى مع المخاطر السيبرانية أم لا، لتتمكن من تحديد الأولوية في الاستثمار مع الأمن السيبراني، أم الاستثمار مع الجهات الأخرى.
- **زيادة وعي الموظفين في مجال الأمن السيبراني:** يجب أن تعمل المؤسسة على زيادة وعي الموظفين لفهم مخاطر الهجمات السيبرانية، وتدريبهم للتعامل معها وفقاً لإجراءات خاصة في مجال الأمن السيبراني.
- **نمذجة المخاطر السيبرانية:** يجب على المؤسسة إنشاء نموذج شامل لجميع المخاطر السيبرانية التي تواجهها، وتقييمها سواء أكانت مخاطر خارجية أو داخلية.
- **تطوير المؤسسة لتعاملها مع المخاطر السيبرانية:** يجب على المؤسسة وضع فترات مُحددة ومُنتظمة لمراقبة المخاطر الإلكترونية داخلها، ثم تقييمها وتحليل جميع بياناتها، وإنشاء خطة لتحسينها، ثم تقديم تقرير شامل لمجلس الإدارة يُوضّح وضع المخاطر الإلكترونية عبر المؤسسة، ومستوى تطبيقها لضوابط الأمن السيبراني.



٢. تعزيز الأمن السيبراني

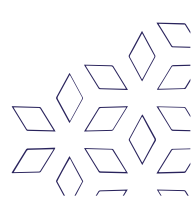
- **إدارة الأصول:** للتأكد من أن الجهة لديها قائمة جرد دقيقة وحديثة للأصول تشمل التفاصيل ذات العالقة لجميع الأصول المعلوماتية والتقنية المتاحة للجهة، من أجل دعم العمليات التشغيلية للجهة ومتطلبات الأمن السيبراني، لتحقيق سرية وسلامة الأصول المعلوماتية، والتقنية للجهة، ودقتها، وتوافره.
- **إدارة هويات الدخول والصلاحيات:** ضمان حماية الأمن السيبراني للوصول المنطقي Access Logical إلى الأصول المعلوماتية والتقنية للجهة من أجل منع الوصول غير المصرح به وتقييد الوصول إلى ما هو مطلوب لإنجاز الأعمال المتعلقة بالجهة.
- **حماية الأنظمة وأجهزة معالجة المعلومات:** ضمان حماية الأنظمة وأجهزة معالجة المعلومات بما في ذلك أجهزة المستخدمين والبنى التحتية للجهة من المخاطر السيبرانية، **يجب أن تغطي متطلبات الأمن السيبراني لحماية الأنظمة وأجهزة معالجة المعلومات للجهة بحد أدنى ما يلي:**
    - الحماية من الفيروسات والبرامج والأنشطة المشبوهة والبرمجيات الضارة (Malware) على أجهزة المستخدمين والخوادم باستخدام تقنيات وآليات الحماية الحديثة والمتقدمة، وإدارتها بشكل آمن.
    - التقييد الحازم الاستخدام أجهزة وسائط التخزين الخارجية والأمن المتعلق بها.
    - إدارة حزم التحديثات والإصلاحات للأنظمة والتطبيقات والأجهزة Patch Management.
    - مزامنة التوقيت (Clock Synchronization) مركزياً ومن مصدر دقيق وموثوق، ومن هذه المصادر ما توفره الهيئة السعودية للمواصفات والمقاييس والجودة.



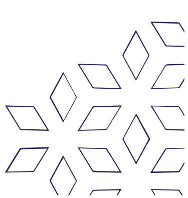
○ حماية البريد الإلكتروني:

ضمان حماية البريد الإلكتروني للجهة من المخاطر السيبرانية.

- تحليل وتصفية (Filtering) رسائل البريد الإلكتروني وخصوصاً رسائل التصيد الإلكتروني (Emails Phishing) والرسائل الاقتحامية (Emails Spam) باستخدام تقنيات وآليات الحماية الحديثة والمتقدمة للبريد الإلكتروني .
- التحقق من الهوية متعدد العناصر (Authentication Factor-Multi) للدخول عن بعد والدخول عن طريق صفحة موقع البريد الإلكتروني (Webmail).
- النسخ الاحتياطي والأرشفة للبريد الإلكتروني
- الحماية من التهديدات المتقدمة المستمرة (APT Protection)، التي تستخدم عادة الفيروسات والبرمجيات الضارة غير المعروفة مسبقاً (Day-Zero Malware)، وإدارتها بشكل آمن.
- توثيق مجال البريد الإلكتروني للجهة بالطرق التقنية، مثل طريقة إطار سياسة المرسل Sender Police Framework



- **إدارة أمن الشبكات: يجب أن تغطي متطلبات الأمن السيبراني لإدارة أمن شبكات الجهة بحد أدنى ما يلي:**
  - العزل والتقسيم المادي أو المنطقي لأجزاء الشبكات بشكل آمن، واللازم للسيطرة على مخاطر الأمن السيبراني ذات العلاقة، باستخدام جدار الحماية Firewall ومبدأ الدفاع الأمني متعدد المراحل (Defense-in-Depth).
  - عزل شبكة بيئة الإنتاج عن شبكات بيئات التطوير والاختبار .
  - أمن التصفح والاتصال بالإنترنت، ويشمل ذلك التقييد الحازم للمواقع الإلكترونية المشبوهة، ومواقع مشاركة وتخزين الملفات، ومواقع الدخول عن بعد .
  - أمن الشبكات اللاسلكية وحمايتها باستخدام وسائل آمنة للتحقق من الهوية والتشفير، وعدم على دراسة متكاملة للمخاطر المترتبة ً ربط الشبكات اللاسلكية بشبكة الجهة الداخلية إلا بناء على ذلك والتعامل معها بما يضمن حماية الأصول التقنية للجهة.
  - قيود وإدارة منافذ وبروتوكولات وخدمات الشبكة.
  - أنظمة الحماية المتقدمة لاكتشاف ومنع الإختراقات Intrusion Prevension System
  - أمن نظام أسماء النطاقات DNS.
  - حماية قناة تصفح الإنترنت من التهديدات المتقدمة المستمرة APT Protection، التي تستخدم عادة الفيروسات والبرمجيات الضارة غير المعروفة مسبقاً Zero-Day malware.



- **أمن الأجهزة المحمولة:**

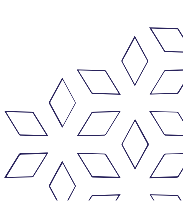
ضمان حماية أجهزة الجهة المحمولة (بما في ذلك أجهزة الحاسب المحمول والهواتف الذكية والأجهزة الذكية اللوحية) من المخاطر السيبرانية، وضمان التعامل بشكل آمن مع المعلومات الحساسة والمعلومات الخاصة بأعمال الجهة وحمايتها أثناء النقل والتخزين عند استخدام الأجهزة الشخصية للعاملين في الجهة.

يجب أن تغطي متطلبات الأمن السيبراني الخاصة بأمن الأجهزة المحمولة وأجهزة (BYOD) للجهة بحد أدنى ما يلي:

- فصل وتشفير البيانات والمعلومات الخاصة بالجهة المخزنة على الأجهزة المحمولة وأجهزة.BYOD
- الاستخدام المحدد والمقيد بناء على ما تتطلبه مصلحة أعمال الجهة.
- حذف البيانات والمعلومات الخاصة بالجهة المخزنة على الأجهزة المحمولة وأجهزة (BYOD) عند فقدان الأجهزة أو بعد انتهاء/إنهاء العلاقة الوظيفية مع الجهة.
- التوعية الأمنية للمستخدمين.

- **حماية البيانات والمعلومات:**

- ضمان حماية السرية وسلامة بيانات ومعلومات الجهة ودقتها وتوافرها، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.
- ملكية المعلومات والبيانات.
- تصنيف البيانات والمعلومات وآلية ترميزها.
- خصوصية البيانات والمعلومات.



- **التشفير cryptography:**

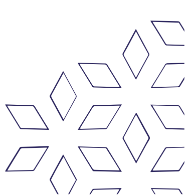
ضمان الاستخدام السليم والفعال للتشفير لحماية الأصول المعلوماتية الإلكترونية للجهة، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة مثل:

- معايير حلول التشفير المعتمدة والقيود المطبقة عليها (تقنياً وتنظيمياً).
- الإدارة الآمنة لمفاتيح التشفير خلال عمليات دورة حياتها.
- تشفير البيانات أثناء النقل والتخزين بناء على تصنيفها وحسب المتطلبات التشريعية والتنظيمية ذات العلاقة.

- **إدارة النسخ الإحتياطية:**

ضمان حماية بيانات ومعلومات الجهة والإعدادات التقنية للأنظمة والتطبيقات الخاصة بالجهة من الأضرار الناجمة عن المخاطر السيبرانية، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة مثل:

- نطاق النسخ الاحتياطية وشموليتها للأصول المعلوماتية والتقنية الحساسة.
- القدرة السريعة على استعادة البيانات والأنظمة بعد التعرض لحوادث الأمن السيبراني.
- إجراء فحص دوري لمدى فعالية استعادة النسخ الاحتياطية.



- **إدارة الثغرات:**

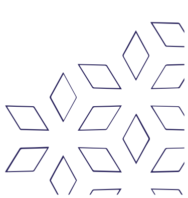
ضمان اكتشاف الثغرات التقنية في الوقت المناسب ومعالجتها بشكل فعال، وذلك لمنع أو تقليل احتمالية الهدف استغلال هذه الثغرات من قبل الهجمات السيبرانية وتقليل الآثار المترتبة على أعمال الجهة وذلك من خلال:

- فحص واكتشاف الثغرات دورياً.
- تصنيف الثغرات حسب خطورتها
- معالجة الثغرات بناءا على تصنيفها والمخاطر السيبرانية المترتبة عليها
- إدارة حزم التحديثات والإصلاحات الأمنية لمعالجة الثغرات.
- التواصل والاشتراك مع مصادر موثوقة فيما يتعلق بالتنبيهات المتعلقة بالثغرات الجديدة والمحدثة

- **اختبار الإختراق:**

تقييم واختبار مدى فعالية قدرات تعزيز الأمن السيبراني في الجهة، وذلك من خلال عمل محاكاة لتقنيات وأساليب الهجوم السيبراني الفعلية، ولاكتشاف نقاط الضعف الأمنية غير المعروفة والتي قد تؤدي إلى الاختراق السيبراني للجهة، وذلك وفقاً للمتطلبات التشريعية والتنظيمية ذات العالقة.

- نطاق عمل اختبار الاختراق، ليشمل جميع الخدمات المقدمة خارجياً(عن طريق الإنترنت) ومكوناتها التقنية، ومنها: البنية التحتية، المواقع الإلكترونية، تطبيقات الويب، تطبيقات الهواتف الذكية واللوحية، البريد الإلكتروني والدخول عن بعد.
- عمل اختبار الاختراق دورياً.



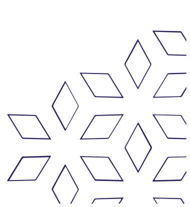
- **إدارة سجلات الأحداث ومراقبة الأمن السيراني:**

ضمان تجميع وتحليل ومراقبة سجلات أحداث الأمن السيبراني في الوقت المناسب من أجل الاكتشاف الاستباقي للهجمات السيبرانية وإدارة مخاطرها بفعالية لمنع أو تقليل الآثار المترتبة على أعمال الجهة

- تفعيل سجلات الأحداث (logs Event) الخاصة بالأمن السيبراني على الأصول المعلوماتية الحساسة لدى الجهة.
- تفعيل سجالا الأحداث الخاصة بالحسابات ذات الصلاحيات الهامة والحساسة على الأصول المعلوماتية وأحداث عمليات الدخول عن بعد لدى الجهة.
- تحديد التقنيات اللازمة (SIEM) لجمع سجلات الأحداث الخاصة بالأمن السيبراني.
- المراقبة المستمرة لسجلات الأحداث الخاصة بالأمن السيبراني.
- مدة الاحتفاظ بسجلات الأحداث الخاصة بالأمن السيبراني (على ألا تقل عن ١٢ شهر).

- **إدارة حوادث وتهديدات الأمن السيبراني**

- ضمان تحديد واكتشاف حوادث الأمن السيبراني في الوقت المناسب وإدارتها بشكل فعال والتعامل مع تهديدات الأمن السيبراني استباقياً من أجل منع أو تقليل الآثار المترتبة على أعمال الجهة.
- وضع خطط الاستجابة للحوادث الأمنية وآليات التصعيد.
- تصنيف حوادث الأمن السيبراني.
- تبليغ الهيئة عند حدوث حادثة أمن سيبراني.
- مشاركة التنبيهات والمعلومات الاستباقية ومؤشرات الاختراق وتقارير حوادث الأمن السيبراني مع الهيئة.
- الحصول على المعلومات الاستباقية (Intelligence Threat) والتعامل معها.



○ **الأمن المادي:**

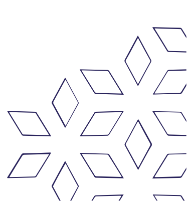
ضمان حماية الأصول المعلوماتية والتقنية للجهة من الوصول المادي غير المصرح به والفقدان والسرقة والتخريب

- الدخول المصرح به للأماكن الحساسة في الجهة مثل مركز بيانات الجهة، مركز التعافي من الكوارث، أماكن معالجة المعلومات الحساسة، مركز المراقبة الأمنية، غرف اتصالات الشبكة، مناطق الإمداد الخاصة بالأجهزة والعتاد التقنية، وغيرها.
- سجلات الدخول و المراقبة CCTV.
- حماية معلومات سجلات الدخول والمراقبة
- أمن إتلاف وإعادة استخدام الأصول المادية التي تحوي معلومات مصنفة وتشمل الوثائق الورقية ووسائط الحفظ والتخزين.
- أمن الأجهزة والمعدات داخل مباني الجهة وخارجها

○ **حماية تطبيقات الويب:**

يجب تحديد وتوثيق واعتماد متطلبات الأمن السيبراني لحماية تطبيقات الويب الخارجية للجهة من المخاطر السيبرانية

- استخدام جدار الحمايةلتطبيقات الويب webApplication Firewall.
- استخدام مبدأ المعمارية متعددة المستويات Multi-tier Architecture .
- استخدام بروتوكولات أمنة مثل بروتوكول https .
- توضيح سياسة الاستخدام الآمن للمستخدمين.
- التحقق من الهوية متعدد العناصر Multi-factor authentication لعمليات دخول المستخدمين.



٣. صمود الأمن السيبراني

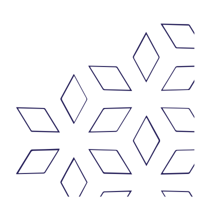
- ضمان توافر متطلبات صمود الأمن السيبراني في إدارة استمرارية أعمال الجهة، وضمان معالجة وتقليل الآثار المترتبة على الاضطرابات في الخدمات الإلكترونية الحرجة للجهة وأنظمة وأجهزة معالجة معلوماتها جراء الكوارث الناتجة عن المخاطر السيبرانية.
- التأكد من استمرارية الأنظمة والإجراءات المتعلقة بالأمن السيبراني.
- وضع خطط الاستجابة لحوادث الأمن السيبراني التي قد تؤثر على استمرارية أعمال الجهة.
- وضع خطط التعافي من الكوارث Disaster Recovery Plan.

٤. الأمن السيبراني المتعلق بالأطراف الخارجية

ضمان حماية أصول الجهة من مخاطر الأمن السيبراني المتعلقة بالأطراف الخارجية، بما في ذلك خدمات الإسناد لتقنية المعلومات Outsourcing والخدمات المدارة Managed Services، وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية ذات العلاقة.

كما يجب أن تغطي متطلبات الأمن السيبراني ضمن العقود والاتفاقيات مثل اتفاقية مستوى الخدمة SAL مع الأطراف الخارجية التي قد تتأثر بإصابتها بيانات الجهة أو الخدمات المقدمة لها بحد أدنى ما يلي:

- بنود المحافظة على سرية المعلومات (Non-Disclosure Clauses) والحذف الآمن من قِبل الطرف الخارجي لبيانات الجهة عند انتهاء الخدمة.
- إجراءات التواصل في حال حدوث حادثة أمن سيبراني.
- إلزام الطرف الخارجي بتطبيق متطلبات وسياسات الأمن السيبراني للجهة والمتطلبات التشريعية والتنظيمية ذات العلاقة.



٥. الأمن السيبراني المتعلق بالحوسبة السحابية والإستضافة

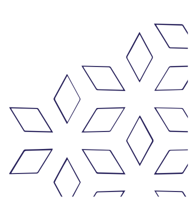
ضمان معالجة المخاطر السيبرانية وتنفيذ متطلبات الأمن السيبراني للحوسبة السحابية والاستضافة بشكلٍ ملائم وفعال، وذلك وفقاً للسياسات والإجراءات التنظيمية للجهة، والمتطلبات التشريعية والتنظيمية والأوامر والقرارات ذات العالقة، وضمان حماية الأصول المعلوماتية والتقنية للجهة على خدمات الحوسبة السحابية التي تتم استضافتها أو معالجتها أو إدارتها بواسطة أطراف خارجية

- تصنيف البيانات قبل استضافتها لدى مقدمي خدمات الحوسبة السحابية والاستضافة، وإعادتها للجهة بصيغة قابلة للاستخدام عند انتهاء الخدمة.
- فصل البيئة الخاصة بالجهة وخصوصاً الخوادم الافتراضية عن غيرها من البيئات التابعة لجهات أخرى في خدمات الحوسبة السحابية.
- موقع استضافة وتخزين معلومات الجهة يجب أن يكون داخل المملكة.

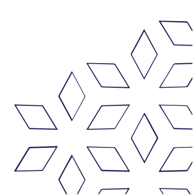
٦. الأمن السيبراني لأنظمة التحكم الصناعي

ضمان إدارة الأمن السيبراني بشكل سليم وفعال لحماية توافر وسالمة وسرية أصول الجهة المتعلقة بأجهزة وأنظمة التحكم الصناعي (ICS/OT) ضد الهجوم السيبراني مثل الوصول غير المصرح به والتخريب والتجسس والتلاعب بما يتماشى مع إستراتيجية الأمن السيبراني للجهة، وإدارة مخاطر الأمن السيبراني، والمتطلبات التشريعية والتنظيمية ذات العلاقة وكذلك المتطلبات الدولية المقرة تنظيمياً على الجهة والمتعلقة بالأمن السيبراني

- التقييد الحازم والتقسيم المادي والمنطقي عند ربط شبكات الإنتاج الصناعية (ICS/OT) مع الشبكات الأخرى التابعة للجهة، مثل: شبكة الأعمال الداخلية للجهة "Corporate Network".



- التقييد الحازم والتقسيم المادي والمنطقي عند ربط الأنظمة أو الشبكات الصناعية مع شبكات خارجية، مثل: الإنترنت أو الدخول عن بعد أو الاتصال اللاسلكي.
- تفعيل سجلات الأحداث (Event logs) الخاصة بالأمن السيبراني للشبكة الصناعية والاتصالات المرتبطة بها ما أمكن ذلك، والمراقبة المستمرة لها.
- عزل أنظمة معدات السلامة.
- التقييد الحازم لاستخدام وسائط التخزين الخارجية.
- التقييد الحازم لتوصيل الأجهزة المحمولة على شبكة الإنتاج الصناعية.
- مراجعة إعدادات وتحصين الأنظمة الصناعية، وأنظمة الدعم والأجهزة الآلية الصناعية (Secure Configuration and Hardening) دورياً.
- إدارة ثغرات الأنظمة الصناعية.
- إدارة حـزم الـتـحـديـثـات والإصلاحات الأمنية للأنظمة الـصـنـاعـيـة.
- إدارة البرامج الخاصة بالأمن السيبراني الصناعي للحماية من الفيروسات والبرمجيات المشبوهة والضارة.

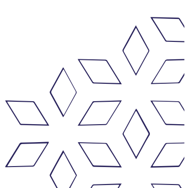


❖ اللوائح والقوانين المتعلقة بالأمن السيبراني

كثيرا ما نسمع في الآونة الأخيرة مصطلحات لم تكن موجودة سابقاً في عالم القانون، مثل قوانين الجرائم المعلوماتية، قوانين الخصوصية الرقمية، قوانين الفضاء السيبراني، ويستتبعه مفاهيم حديثة مثل مفهوم الحوكمة السيبرانية، والتي لازال الكثير يعاني في فهم أسلوب تطبيقها، ظهر مفهوم الجرائم السيبرانية الزيادة في استخدام التجارة الإلكترونية والتي دعت الى وجود ممارسات تنظيمية مناسبة لضمان عدم حدوث ممارسات خاطئة تسلب المتعاملين رقميا من حقوقهم، لذلك، كان أول قانون إلكتروني موجود على الإطلاق في أمريكا، ويطلق عليه قانون الاحتيال وإساءة استخدام الكمبيوتر، والذي أصدر في عام ١٩٨٦. هدف هذا القانون الى حظر الوصول غير المصرح به إلى أجهزة الكمبيوتر والاستخدام غير القانوني للمعلومات الرقمية.

يشار إلى قانون الأمن السيبراني أو قانون تكنولوجيا المعلومات باسم قانون الإنترنت، وهذا يعني أنه يمكن تعريف قانون الأمن السيبراني بأنه نظام قانوني مصمم للتعامل مع الإنترنت والحوسبة والفضاء السيبراني والقضايا القانونية ذات الصلة، بمعنى اخر، الوصف الملائم لقانون الإنترنت هو: إيجادقوانين ورقية لتنظم العالم اللاورقي.

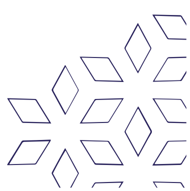
وعندما نشير الى قانون الأمن السيبراني، لايعني ذلك أننا نقصد الجرائم فقط التي يمكن أن ترتكب من خلال هذا الفضاء، وإنما تشكل جوانب الملكية الفكرية، والعقود، والولاية القضائية، وقوانين حماية البيانات والخصوصية وحرية التعبير، كما يشمل أيضا التداول الرقمي للبرامج والتطبيقات والمعلومات والتجارة الإلكترونية وكل ما يتعلق بحماية الحقوق وتوفير الأمن الرقمي، يوفر مجال القانون السيبراني الاعتراف القانوني بالوثائق الإلكترونية، كما أنه ينشئ هيكلاً لمعاملات التجارة الإلكترونية.



تختلف القوانين المطبقة للأمن السيبراني إلى حد كبير من دولة إلى أخرى ومن ولاية قضائية لولاية قضائية أخرى، وتتراوح العقوبات المفروضة على نفس العقوبة أيضاً من الغرامة إلى السجن بناءً على الجريمة المرتكبة على حسب قانون الدولة، لذلك، من المهم جداً أن يعرف المواطنون قوانين الإنترنت في بلدانهم للتأكد من أنهم على دراية جيدة بجميع المعلومات المتعلقة بالأمن السيبراني، وتماماً مثل أي قانون آخر، يتكون قانون الإنترنت من قواعد تحدد كيفية استخدام الأشخاص والشركات للإنترنت وأجهزة الحاسوب، بينما تحمي القواعد الأخرى الأشخاص من الوقوع في شرك الجرائم الإلكترونية والتي تدار من قبل عصابات رقمية، على الرغم من أنه من شبه المستحيل كبح ١٠٠٪ من جميع الجرائم الإلكترونية، فإن القوانين المطبقة في جميع أنحاء العالم تساعد في حماية الحقوق المختلفة التي تتم من خلال القضاء السيبراني.

لذلك تكمن اهمية القوانين السيبرانية في إنها:

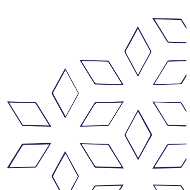
- **أولاً:** تفرض إجراءات للاستخدام وتقيس ردود الفعل العام في الفضاء السيبراني.
- **ثانياً:** ترتفع نسبة الأمان والحماية للمعاملات التي تجرى عبر الإنترنت.
- **ثالثاً:** تخضع جميع الأنشطة عبر الإنترنت للمراقبة من قبل مسؤولي القانون السيبراني.
- **رابعاً:** توفير الحماية لجميع البيانات والممتلكات الخاصة بالأفراد والمنظمات والحكومة.
- **خامساً:** يساعد في الحد من الأنشطة السيبرانية غير القانونية من خلال بذل الرقابة والعناية الواجبة من قبل مؤسسات الدولة المختصة.
- **سادساً:** ردود الفعل التي يتم قياسها على أي فضاء إلكتروني لها زاوية قانونية مرتبطة بها تختلف باختلاف توجهها، سواء كان يتعلق بالتجارة أو بالخدمات او الامن ... الخ.



- **سابعاً:** وجود قوانين سيبرانية يعني وجود اتفاقيات دولية في هذا المجال مما يتيح تتبع جميع السجلات الإلكترونية من خلال تحقيق التعاون الدولي لتتبع الجرائم المنظمة.
- **ثامناً:** يساعد على إنشاء الحوكمة الإلكترونية والتي بدورها ترفع جودة حياة المستفيدين من خدمات الحكومة الالكترونية.

تعريف اللوائح: هي لوائح تشتمل على توجيهات متخصصة لحماية تقنية المعلومات وأنظمة الحاسب بغرض إجبار الشركات والمؤسسات على حماية أنظمتها ومعلوماتها من الهجمات الإلكترونية مثل الفيروسات والديدان وأحصنة طروادة والتصيد وهجمات رفض الخدمة (DOS) والوصول غير المصرح به كسرقة الملكية الفكرية أو المعلومات السرية وهجمات نظام التحكم وغيرها، هناك العديد من التدابير المتاحة لمنع الهجمات الإلكترونية.

تشمل هذه التدابير في الأمن السيبراني بناء سياسات وضوابط وأنظمة مثل إنشاء جدران الحماية وبرامج مكافحة الفيروسات وأنظمة كشف التسلل والوقاية منها والتشفير وكلمات المرور في عمليات تسجيل الدخول، كانت ولازالت هناك محاولات لتحسين الأمن السيبراني من خلال التنظيم والجهود التعاونية بين الحكومة والقطاع الخاص لتشجيع التحسينات الطوعية للأمن السيبراني، لاحظ مسؤولين ومنظمين الصناعة، بما في ذلك المنظمون والشركاء المصرفيون المخاطر الناجمة عن الأمن السيبراني وبدأوا يخططون للبدء في إدراج الأمن السيبراني كجانب من جوانب الاختبارات التنظيمية.



❖ الأطراف المعنية بتنفيذ القواعد التي يجب الالتزام بها

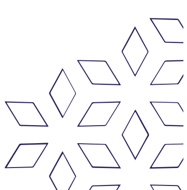
- **نظام مكافحة الجرائم المعلوماتية:**

يهدف نظام مكافحة الجرائم المعلوماتية للحد من الجرائم المعلوماتية بهدف تحديد الجرائم والعقوبات المترتبة عليها، وذلك للمساعدة في تحقيق أمن المعلومات، وحماية المصلحة العامة والأخلاق، وحفظ الحقوق المترتبة على الاستخدام المشروع للحاسبات الآلية والشبكات المعلوماتية وحماية الاقتصاد الوطني.

- **البرامج والمبادرات الوطنية**

١. **المركز الوطني الإرشادي للأمن السيبراني:** من أجل رفع مستوى الوعي بالأمن السيبراني وتجنب المخاطر السيبرانية وتقليل آثارها أطلِق المركز الوطني الإرشادي للأمن السيبراني ليعمل على إصدار التنبيهات بآخر وأخطر الثغرات، كما يعمل على إطلاق حملات وبرامج توعوية، والتعاون مع المراكز الإرشادية الأخرى.

٢. **الاتحاد السعودي للأمن السيبراني والبرمجة والدرونز:** من أجل قدرات محلية احترافية في الأمن السيبراني وتطوير البرمجيات والدرونز أطلِق الاتحاد السعودي للأمن السيبراني والبرمجة والدرونز تحت مظلة اللجنة الأولمبية السعودية للعمل على تقديم أنشطة وبرامج تساهم في زيادة وعي المجتمع بالأمن السيبراني والبرمجة والدرونز ودعم وتشجيع الشباب للاحتراف في هذا المجال.

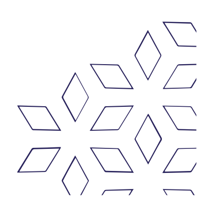


٣. **الأكاديمية الوطنية للأمن السيبراني:** مبادرة أطلقتها وزارة الاتصالات وتقنية المعلومات بالتعاون مع صندوق تنمية الموارد البشرية (هدف) لرفع مستوى القدرات الرقمية الوطنية في مختلف مجالات التقنية الحديثة لمواكبة متطلبات التحول الرقمي، **وتشمل عدّة مسارات:**

- تحليل بيانات الذكاء الاصطناعي
- الحوسبة السحابية
- تطوير الويب والتطبيقات
- تصميم وتطوير الألعاب
- البرامج التنفيذية

٤. **مبادرة حصين:** أطلِقت مبادرة حصين من أجل تعزيز الأمن السيبراني على المستوى الوطني وتُعنى بحماية البريد الإلكتروني من الانتحال والاستخدام الغير مصرح به، **فهي تعمل على تمكين الجهات من:**

- معرفة مستوى تطبيق مبادرة حصين للجهة
- إنشاء سجلات أسماء النطاق
- استطلاع لسجلات أسماء النطاق
- توعية الجهات الوطنية بأهمية تفعيل توثيق أسماء للنطاقات وطرق تنفيذها.

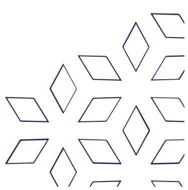


❖ المعايير العالمية للأمن السيبراني

مما لا شك فيه أن أمن المعلومات تلعب دوراً مهما في حماية أصول الشركة أو المؤسسة، و كثيراً ما نسمع في الاخبار عن الحوادث الأمنية لأمن المعلومات، مثل تشويه المواقع، وقرصنة الخادم ، وتسرب البيانات، و لذلك المنظمات بحاجة ماسة إلى أن تدرك الحاجة إلى تكريس المزيد من الموارد لحماية أصول المعلومات، وأمن المعلومات يجب أن يصبح مصدر قلق كبير في كل من الحكومة وقطاع الأعمال، وبما أنه لايمكن أن نضمن حماية للمؤسسة أو الشركة بنسبة ١٠٠%، لذلك نحن بحاجة لوضع مجموعة من المقاييس أو المعايير التي يمكن من خلالها تحقيق مستوى ملائم من الأمن، ومن خلال هذه المقدمة فإننا سنذكر أهم المعايير العالمية التي تساعد على تحقيق الحد الأدنى لأمن المعلومات، **مثل:** الآيزو ISO والكوبيت COBIT و ITIL وكذلك بعض القوانين المرتبطة بأمن المعلومات **مثل:** HIPAA, COSO, SOX FISMA.

- **معاييرالايزو**

المنظمة الدولية للتوحيد القياسي آيزو (ISO) الذي أنشأ في عام ١٩٤٧، هو هيئة غير حكومية تتعاون مع اللجنة الدولية الكهرتقنية (IEC) والاتحاد الدولي للاتصــالات (ITU) على تكنولوجيا المعلومات والاتصالات (ICT)، **وهنا أشهر المعايير التابعة لها:**



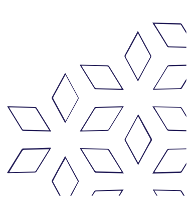
١- أيزو ٢٧٠٠٢:

هذا المعيار يتضمن بعض السياسات والتوجيهات، منها:

- السياسة الأمنية policy Security
- تنظيم أمن المعلومات security information of Organization
- إدارة الأصول management Asset
- أمن الموارد البشرية security resources Human
- الأمن البيئي والمادي security environmental and Physica
- الاتصالات وإدارة العمليات management operations and Communications
- التحكم في الوصول control access
- اقتناء نظم المعلومات وتطويرها وصيانتها development acquisition systems Information and maintenance
- إدارة الحوادث الأمنية للمعلومات management incident security Information
- إدارة استمرارية الأعمال management continuity Business
- إدارة الامتثال أو التوافق management Complianc

٢- أيزو ٢٧٠٠١

هذا المعيار يقدم نموذج دوري يعرف بـ (PDCA) وهو اختصار لـ (Plan-Do-check-Act) ويهدف إلى تحديد الاحتياجات اللازمة لإقامة وتنفيذ وتشغيل ورصد واستعراض وصيانة وتحسين وتوثيق نظام إدارة أمن المعلومات داخل المنظمة، وعادة ما ينطبق على جميع أنواع المنظمات، بما في ذلك المؤسسات التجارية والوكالات الحكومية، وغيرها.



وكما ذكرنا فإن هذا النموذج يتم في أربع مراحل متتابعة:

- الخطة (Plan): تأسيس نظام لإدارة أمن المعلومات.
- التنفيذ (Do): البدء في تنفيذ الخطط وتشغيلها.
- التحقق (Check): مراجعة النظام بعد تنفيذه.
- العمل (Act): صيانة وتحسين النظام.

٣- **<u>أيزو ١٥٤٠٨</u>**

يساعد هذا المعيار على التقييم، والتحقق، والتصديق على الضمانات الأمنية للمنتجات التكنولوجية، وكذلك يمكن تقييم الأجهزة والبرمجيات لمكافحة تغير المناخ في مختبرات معتمدة للتصديق.

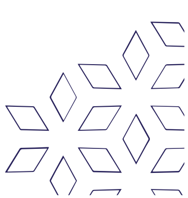
٤- **<u>أيزو ١٣٣٣٥</u>: يتكون من سلسلة من المبادئ والتوجيهات وهي:**

أ – **آيزو ١٣٣٣٥–١** :عبارة عن توثيق للمفاهيم والنماذج لإدارة أمن تكنولوجيا المعلومات والاتصالات.

ب – **-آيزو ١٣٣٣٥–٣:** عبارة عن توثيق للتقنيات لإدارة أمن تكنولوجيا المعلومات.

ج – **آيزو ١٣٣٣٥–٤**: يشمل أختيار الضمانات، كالضوابط الأمنية التقنية.

د – **آيزو ١٣٣٣٥–٥**: يشمل على التوجيه الإداري لأمن الشبكات.



- **معيار الكوبيت COBIT : The Control Objectives for Information and related Technology**

هو عبارة عن إطار للسيطرة أو التحكم تربط تقنية المعلومات بمتطلبات العمل، وتنظيم لأنشطة تكنولوجيا المعلومات في نموذج العملية المقبولة، وتحديد الموارد الرئيسية لتكنولوجيا المعلومات، وأهداف الرقابة الإدارية التي سينظر فيها وقد تم بناء هذا المعيار من قبل معهد حوكمة تقنية المعلومات Institute Governance IT (ITIG) في عام ١٩٩٥م.

وهو الآن في النسخة الرابعة، وتتكون من سبعة أجزاء رئيسية:

١- النظرة التنفيذية: Executive Overview

٢- إطار الكوبيت COBIT Frame work

٣- التخطيط والتنظيم Plan and Organize

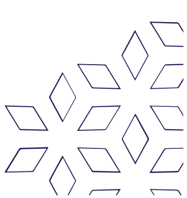
٤- الاكتساب والتنفيذ Acquire and Implement

٥- التسليم والدعم Deliver and Support

٦- الرصد والتقييم Monitor and Evaluate

٧- الملاحق بما في ذلك المعجم أو المصطلحات Appendices

و الكوبيت هو مجموعة من المواد التوجيهية الدولية تستخدم لحوكمة تقنية المعلومات و كذلك تتيح للمديرين سد الفجوة بين متطلبات الرقابة والقضايا التقنية والمخاطر التجارية، واستناداً إلى أبرز النقاط في الكوبيت تبين أنه يركز على مخاطر محددة حول أمن تكنولوجيا المعلومات بطريقة بسيطة لمتابعة وتنفيذ المنظمات الصغيرة والكبيرة.

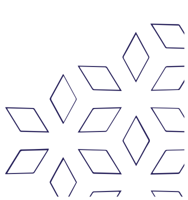


- **معيار ITIL**

هو اختصار لـThe Information Technology Infrastructure Library ويعرف أيضاً بأنه ISO-2000 وهو عبارة عن مجموعة من أفضل الممارسات في مجال إدارة خدمات تقنية المعلومات (ITSM) ويركز على خدمة عمليات تقنية المعلومات ويعتبر الدور الرئيسي للمستخدم.

وقد تم بناؤه بواسطة مكتب المملكة المتحدة لتجارة الحكومة (OGC) وإدارة خدمة التقييم الذاتي بالحكومة حيث يتم العمل بها عن طريق وضع استبيانات للتقييم الذاتي على الإنترنت **لتساعد على تقييم إدارة المناطق التالية:**

- إدارة مستوى الخدمةManagement Level Servi
- الإدارة المالية Financial Management
- إدارة بناء القدرات Capacity Management
- إدارة استمرارية خدمة Service Continuity Management
- إدارة التوفر Availability Management
- مكتب الخدمات Service Desk
- إدارة الحوادثIncident Management
- إدارة المشكلة Problem Management
- إدارة التكوين Configuration management
- إدارة التغيير Change Management
- إدارة الإصدار Release Management



- **اللوائح والقوانين المتعلقة بأمن المعلومات :**

بما أن هناك بعض المعايير العالمية والمبادئ التوجيهية، وضـــرورة الالتزام بالمبادئ والمعايير التي حددتها تلك المؤسسات أو الهيئات، فإننا سنذكر بعض القوانين واللوئح للولايات المتحدة الأميريكية ومنها HIPAA COSO, SOX FISMA.

<u>قانون ساربينز أوكسلي (Sarbanes-Oxley)SOX</u>

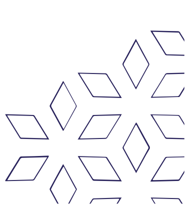
بعد ارتفاع عدد الفضـائح العالية في الولايات المتحدة، بما في ذلك شـركة انرون و وورلدكوم ، صـدر قانون ساربانيس أوكسلي في عام ٢٠٠٢ والغرض من ذلك هو "لحماية المستثمرين عن طريق تحسين دقة وموثوقية نظام الإفصاح أو التعريف المقدمة عملاً لقوانين الأوراق المالية، ولأغراض أخرى" و هذا النظام يؤثر على جميع الشـركات المدرجة في أسـواق الأوراق المالية في الولايات المتحدة ، و قانون SOX يتطلب " كل تقرير سـنوي يحتوي على تقرير للرقابة الداخلية وذلك يتضـمن تقييماً لفاعلية هيكلة وإجراءات المراقبة الداخلية من الجهة المصـدرة لإعداد التقارير المالية" كما تكنولوجيا المعلومات تلعب دورا رئيسـيا في عملية إعداد التقارير المالية والتي السـيطرة عليها سـتكون من الضروري لتقييم معرفة إذا كان قانون SOX تحقق أم لا.

<u>قانون COSO</u>

وهو اختصار Committee Of Sponsoring Organizations of the Tread way Commission

إنه إطار يبدأ من عملية الضوابط الداخلية، كما أنها تساعد على تحسين وسائل السيطرة على الشركات من خلال تقييم فاعلية الضوابط الداخلية، **ويحتوي على خمس مكونات رئيسية:**

- مراقبة البيئة، بما في ذلك عوامل مثل السـلامة من الناس داخل المنظمة وإدارة السـلطة والمسؤوليات
- تقييم المخاطر، وتهدف إلى تحديد وتقييم المخاطر التي يتعرض لها قطاع الأعمال.
- مراقبة الأنشطة، بما في ذلك سياسات وإجراءات لتنظيم.
- المعلومات والاتصـالات، بما في ذلك تحديد المعلومات المهمة لرجال الأعمال وقنوات الاتصال لتقديم قنوات الرقابة من جانب الإدارة للموظفين.
- الرصـد، بما في ذلك عملية اسـتخدامها لرصـد وتقييم جودة جميع نظم الرقابة الداخلية على مر الزمن.



قانون HIPAA:

هو اختصار لـــ The Health Insurance Portability And Accountability Act ويعني قابلية التأمين الصحى وقانون المحاسبة.

هو قانون في الولايات المتحدة يهدف إلى تحسين قابلية واستمرار تغطية التأمين الصحي في المجموعة على حد سواء والأسواق الفردية، ومكافحة الهدر، والاحتيال، وسوء المعاملة في التأمين الصحي والرعاية الصحية، ويحدد القانون معايير الأمنية للحصول على معلومات الرعاية الصحية، ويأخذ في الاعتبار عددا من العوامل بما في ذلك القدرات التقنية لنظم السجلات المستخدمة للحفاظ على المعلومات الصحية، والتكاليف الأمنية، والحاجة لتدريب الموظفين، وقيمة مسارات مراجعة الحسابات في حوسبة نظم السجلات ، واحتياجات وقدرات مقدمي الرعاية الصحية الصغيرة ، و ينبغي حماية المعلومات بشكل صحيح من الأخطار التي تهدد أمن وسلامة هذه المعلومات ، والاستخدامات أو الكشف غير المصرح بها.

قانون FISMA:

هو اختصار لـــ Federal Information Security Management Act ويعني قانون إدارة أمن المعلومات الفيدرالي وهي تتطلب وكالات اتحادية أمريكية لتطوير وتوثيق وتنفيذ برنامج على نطاق الوكالة لتوفير أمن معلومات عن المعلومات (ونظم المعلومات) التي تدعم عمليات الأصول للوكالة، **بعض الاحتياجات ما يلي:**

– تقييم المخاطر الدوري للمعلومات ونظم المعلومات التي تدعم عمليات وأصول المنظمة.

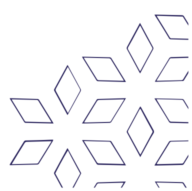
– السياسات والإجراءات للمخاطر إلى دف إلى الحد من مخاطر أمن المعلومات إلى مستوى مقبول.

– التخطيط لتوفير الأمن الكافي لشبكات ونظم المعلومات.

– التدريب على الوعي الأمني لجميع الأفراد، بمن في ذلك المتعاقدون.

– التقييم والاختبار الدوري لفعالية السياسات الأمنية والإجراءات والضوابط.

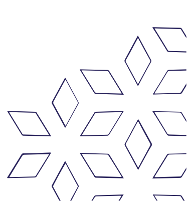
– خطة استمرارية العمل في مكان لدعم عمل المنظمة.



قانون FIPs :

هو اختصار لـ The Federal Information Processing Standards ويعني قانون معايير معالجة المعلومات الفيدرالية، وهو عبارة عن سلسلة من المنشورات الرسمية المتعلقة المعايير والمبادئ التوجيهية المعتمدة والمتاحة والمجالات المتصلة به **ما يلي:**.

- التحكم في الوصول access Control
- التوعية والتدريب awareness and training
- التدقيق والمساءلة audit and accountability
- التصديق، والاعتماد التقييمات الأمنية certification , accreditation and security assessments
- إدارة التكوين Configuration management
- التخطيط للطوارىء contingency planning
- تحديد الهوية والتوثيق identification and authentication
- استجابة الحادث Incident response
- الصيانة maintenance
- حماية وسائل الإعلام media protection
- توفير الحماية المادية والبيئية physical and environmental protection
- التخطيط Planning
- أمن الأفراد personnel security
- تقييم المخاطر risk assessment
- اقتناء نظم الخدمات systems and services acquisition
- حماية نظام الاتصالات systems and communications protection
- النظام وسلامة المعلومات System and Information Integrity



❖ تصنيف المعلومات ومستوياتها

كلمة المعلومات اصطلاحا، فهي تعني البيانات التي تمت معالجتها حتى تصبح لها معنى وأيضا مغزى معين للاستعمالات المحددة، وذلك بهدف اتخاذ القرار، وبتلك الطريقة من الممكن تداولها وأيضا تسجيلها ونشرها وتوزيعها، ويكون ذلك في إطار رسمي او حتى غير رسمي، وذلك لأنها تكون حقيقية يستند اليها الكثير من البحوث العلمية وذلك بعد عدد كبير من المراحل للتنقيب وأيضا للاستقصاء والاستقراء والتجارب والتي تم بناؤها على المناهج العلمية.

- **اشكال وأنواع المعلومات**

١. **المعلومات التطويرية أو الإنمائية:** هي تلك المعلومات التي تعمل على تحسين المستوى العلمي وأيضا الثقافي للشخص، كما انها تعمل على توسيع مداركه بشكل كبير، مثل القراءة للكتب.

٢. **المعلومات الانجازية:** هي المعلومات الخاصة التي تعمل على افادة الانسان في اعماله وأيضا في مشاريعه، او اتخاذ أي قرارات خاصة بها.

٣. **المعلومات التعليمية:** وهي تلك المعلومات التي يتلقاها الطلبة في كل مراحلهم التعليمية الاكاديمية.

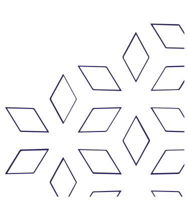
٤. **المعلومات الفكرية:** في تلك الأفكار وأيضا النظريات الفرضية والتي يتم وضعها الانسان حول كل العلاقات التي من الممكن ان تتواجد بين عناصر المشكلة المختلفة.

٥. **المعلومات البحثية:** هي تلك المعلومات التي يتم الحصول عليها من بعض التجارب الشخصية او حتى تجارب الاخرين، وسواء كانت تلك التجارب هي تجارب معملية او حتى تجارب شخصية، او حتى حصيلة تجارب الاخرين من تجارب معملية او أبحاث أدبية، كما تشمل أيضاً التجارب النفسية وعملية اجراءها وأيضا نتيجة الابحاث، والبيانات المطلوبة منها.

٦. **المعلومات الأسلوبية النظامية:** هي المعلومات التي تعمل على مساعدة الباحث على انجاز بحثه بطريقة دقيقة للغاية، كما انه يشمل الوسائل التي تستعمل للحصول على المعلومات وأيضا البيانات الصحيحة.

٧. **المعلومات السياسية:** وهي تلك المواضيع التي تخص كل المواضيع السياسية وأيضا عمليات اتخاذ القرار.

٨. **المعلومات التوجيهية:** هي المعلومات التي يحصل عليها الشخص من خلال توجيه الاخرين له.



❖ التدريب والتوعية بالأمن السيبراني

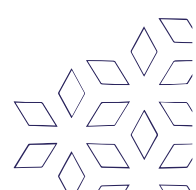
أمن المعلومات مسؤولية جماعية يعد الخطأ البشري في انتهاكات الأمن السيبراني مشكلة قديمة العهد، لذلك يجب على جميع المنظمات أن تظل يقظة وأن تثقف موظفيها للتخفيف من هذه الأخطاء.

من السهل أن نتخيل أن خروقات إنتهاكات الشبكة هي من عمل مجموعات الهاكرز المتطورة، في الواقع، يتم بدء نسبة كبيرة من الانتهاكات باستخدام استراتيجيات هجوم منخفضة التقنية مثل التصيد الاحتيالي والهندسة الاجتماعية، من خلال مطالبة المستخدم النهائي بكشف بيانات اعتماد تسجيل الدخول الخاصة به أو فتح مرفق ضار، يمكن للمهاجمين اختراق الشبكات التي يصعب اختراقها.

"٤٣ ٪ من القادة والمديرين التنفيذيين الذين أبلغوا عن خرق للبيانات في منظماتهم ذكروا أن السبب كان خطأ بشريًا باعتباره السبب الرئيسي الثاني للاختراق"

لذلك يجب على الشركات أن تستثمر باستمرار في دورات تدريبية للتوعية بالأمن السيبراني لجميع موظفيها لأن الأشخاص يمثلون أكبر تهديد لأمن الشبكة.

يمكن لبرامج التدريب تسليح المستخدمين النهائيين بالمهارات اللازمة للتخفيف من التهديدات السيبرانية الشائعة.



رابعاً :أمن الحاسوب والبرمجيات

في هذا الفصل سنتعرف على المواضيع التالية:

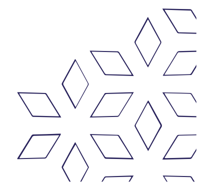
- أمن الحاسوب
- أمن الملفات
- التهديدات الرقمية للحاسبات والبرمجيات (عملي)
- أمن أنظمة التشغيل
- مقارنة بين أنظمة التشغيل من حيث الأمان
- أنظمة حماية قواعد البيانات
- المخاطر الأمنية لنظم قواعد البيانات
- جدران الحماية وأنواعها
- التهديدات الالكترونية الشائعة

❖ أمن الحاسوب

أمن الحاسوب هو فرع من فروع التقانة المعروفة باسم أمن المعلومات، كما هي مطبقة على الحاسوب والشبكات، والهدف من أمن الحاسوب يتضمن حماية المعلومات والممتلكات من السرقة والفساد، أو الكوارث الطبيعية، بينما يسمح للمعلومات والممتلكات أن تبقى منتجة وفي متناول مستخدميها المستهدفين، مصطلحات أمن نظام الحاسوب، تعني العمليات والآليات الجماعية التي من خلالها تُّحمى المعلومات والخدمات الحساسة والقيمة من النشر، والعبث بها أو الانهيار الذي تسببه الأنشطة غير المأذون بها أو الأفراد غير الجديرين بالثقة، والأحداث غير المخطط لها على التوالي.

ممكن تعريف أمن المعلومات بأنه العلم الذي يعمل على توفير الحماية للمعلومات من المخاطر التي تهددها أو الاعتداء عليها وذلك من خلال توفير الادوات والوسائل اللازم توفيرها لحماية المعلومات من المخاطر الداخلية أو الخارجية، المعايير والإجراءات المتخذة لمنع وصول المعلومات إلى أيدي أشخاص غير مخولين عبر الاتصالات ولضمان أصالة وصحة هذه الاتصالات، وإن امن المعلومات هو أمر قديم، ولكن بدا استخدامه بشكل فعلي منذ تطور التقانة

- أنظمة حماية نظم التشغيل
- أنظمة حماية البرامج والتطبيقات
- أنظمة حماية قواعد البيانات
- أنظمة حماية الولوج

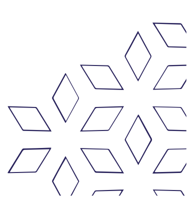


❖ أمن الملفات

الملف هو عبارة عن كائن موجود على جهاز الكمبيوتر، يقوم بتخزين البيانات، أو المعلومات، أو الإعدادات، أو الأوامر المستخدمة في برنامج الكمبيوتر، وفي واجهة المستخدم الرسومية مثل مايكروسوفت ويندوز يتم عرض الملفات على هيئة رموز تتعلق بالبرنامج الذي يفتح هذا اللف، على سبيل المثال تكون أيقونة ملف الصورة مرتبطة ببرنامج أدوبي أكروبات بي دي إف، وعند النقر المزدوج على تلك الأيقونة يفتح برنامج أدوبي أكروبات أو قاريء PDF المثبت على الكمبيوتر.

على الرغم من أن طريقة تعامل البرامج مع الملفات تختلف تبعاً لنظام التشغيل ونظام الملفات المستخدم، **إلا أن العمليات التالية على الملفات شائعة:**

- إنشاء ملف جديد باسم معين
- تغيير خصائص الملف التي تتحكم في العمليات التي تجرى عليه
- فتح ملف واستخدام محتوياته
- قراءة أو تغيير محتويات الملف
- حفظ التعديلات المجراة على الملف
- إغلاق الملف، وبالتالي عدم القدرة على استخدامه إلا بعد فتحه مجدداً



كيفية حماية الملفات

إذا كانت لديك ملفات تفضل ألا يتمكن الآخرون من الوصول إليها، فقد يكون حماية الملفات بكلمة مرور هو أبسط طريقة للحصول على حماية معلوماتك، توجد العديد من الطرق التي يمكنك استخدامها لحماية ملفاتك وتختلف تبعاً لنوع نظام التشغيل الذي تستخدمه ومستوى الحماية الذي تنشده، فمثلاً يحتوي ويندوز على دعم مدمج لحماية ملفاتك بكلمة مرور، مما يتيح لك الحفاظ على ملفاتك في مأمن بعيداً عن أعين المتطفلين، هناك برامج مخصصة لحماية ملفاتك أيضاً وهذا ما سوف نستعرضه تالياً:

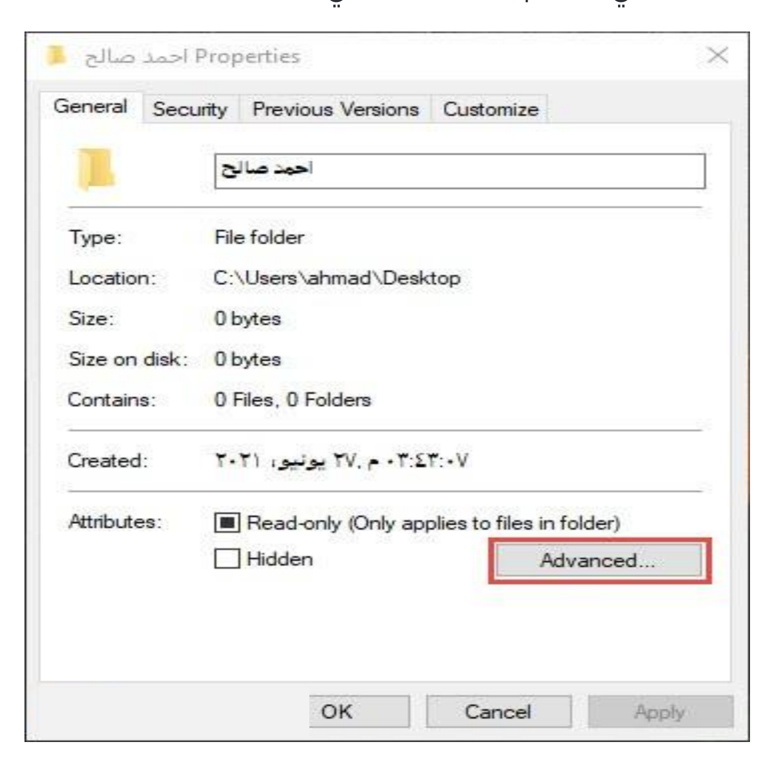
- **حماية الملفات باستخدام ويندوز ١٠**

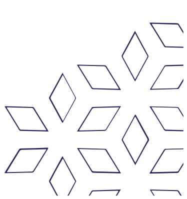
لحماية ملف ما على نظام ويندوز قم باتباع الخطوات التالية:

١- ابحث عن الملف او المجلد الذي تريد حمايته

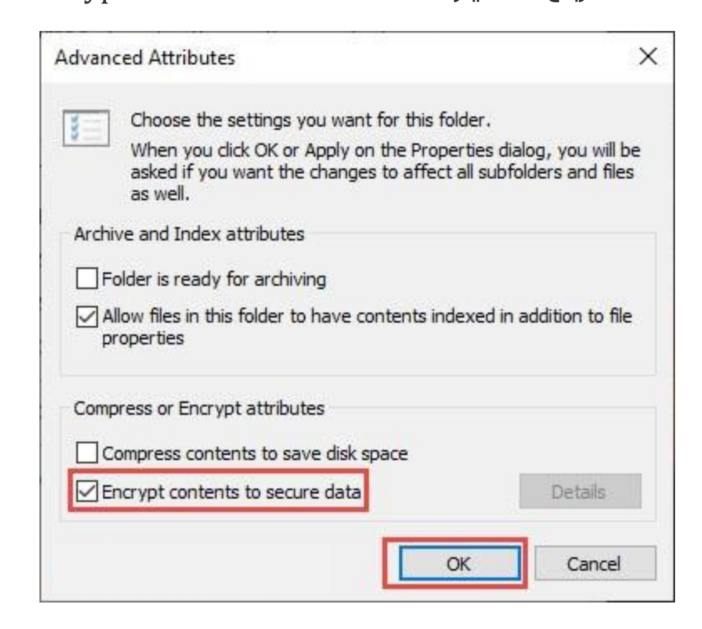
٢- انقر بزر الماوس الأيمن على الملف أو المجلد ثم انقر على Properties أسفل قائمة السياق

٣- انقر على زر ...Advanced في قسم Attributes في النافذة





٤- حدد مربع الاختيار Encrypt contents to secure data



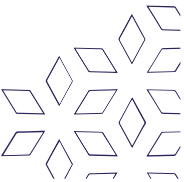
٥- انقر على الزر Ok للعودة إلى نافذة الخصائص الرئيسية.

٦- الآن اضغط على Apply وسيرسل لك ويندوز اشعارًا لبدأ حماية الملفات انقر عليه.

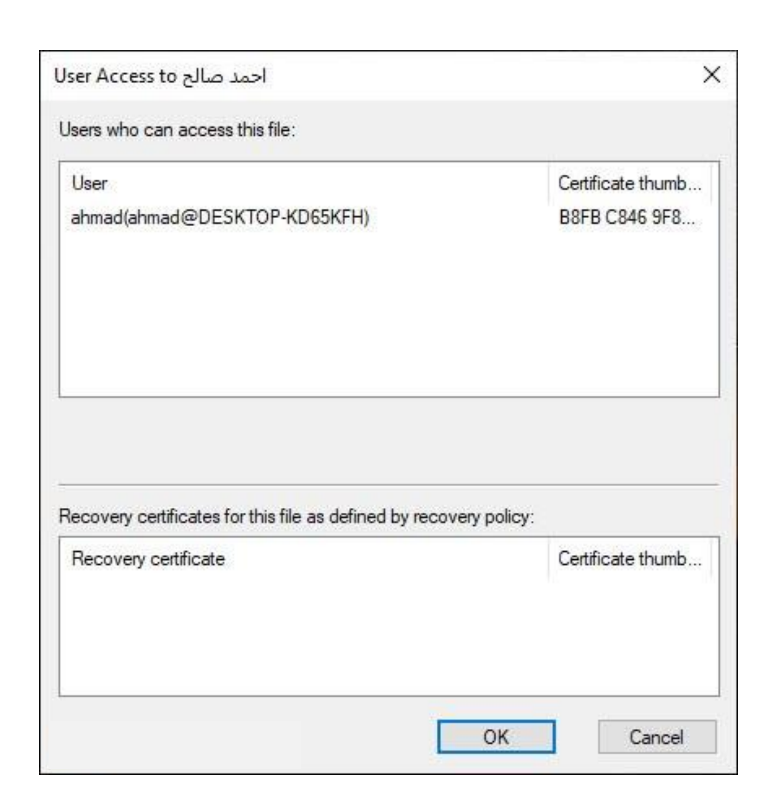
٧- انقر على Back up now لبدأ النسخ الاحتياطي، وتابع الخطوات التي ستظهر على الشاشة.

٨- بعد الإنتهاء من التكوين سيكون لديك ملف احتياطي صغير، ستحتاج إلى هذه المعلومات إذا فقدت الوصول إلى ملفاتك المحمية

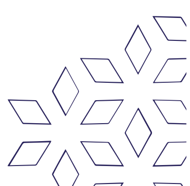




بعد إجراء النسخ الاحتياطي، سيتم الآن حماية الملفات، يتم تشفير هذه الملفات بمفتاح مرتبط بحساب مستخدم ويندوز الخاص بك، يُمكنك التحقق منه بالنقر على Details بجوار زر الاختيار Encrypt contents to secure data.



- إذا حاول أي شخص آخر الوصول إلى الملف – سواء من حساب مستخدم آخر، أو عن طريق إزالة محرك الأقراص الثابتة فعلياً – فستظهر المحتويات على أنها نص مشوه لا معنى له.
- يمكنك فك حماية الملفات في أي وقت بالعودة إلى نافذة Properties وفتح Advanced مرة أخرى.
- فقط قم بإلغاء تحديد مربع الاختيار Encrypt contents to secure data وانقر فوق Ok لإغلاق النوافذ.

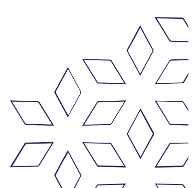


- **كيفية حماية الملفات على جوجل دريف**

- قد لا يسمح لك جوجل دريف بحماية الملفات في مستندات جوجل الفردية، ولكن لا تزال هناك طرق لحماية خصوصيتك.
- قد لا تحتوي مستندات جوجل على خيار لحماية الملفات بكلمة مرور، لكنها لا تزال محمية على خوادم جوجل، ما لم تقم بمشاركتها، فلن يتمكن المستخدمون الآخرون من رؤية ملفاتك بدون اسم المستخدم وكلمة المرور لحساب جوجل الخاص بك.



- لحماية الملفات في جوجل دريف تأكد من أن حسابك آمن قدر الإمكان:
  - استخدم كلمة مرور قوية، وقم بتمكين المصادقة الثنائية.
  - استخدم مفتاح أمان للكمبيوتر مثل Titan أو YubiKey للحصول على أفضل حماية ممكنة.
- إذا قُمت بإعدادا هذه الخطوات بشكل صحيح لن يتمكن أي شخص من الدخول إلى حسابك.



❖ التهديدات الرقمية للحاسبات والبرمجيات (عملي)

البرامج الضارة

يقصد بالبرمجيات الخبيثة هي أي برنامج يعطي بعض السيطرة أو السيطرة الكاملة على الحاسوب الخاص بك لمن قام بتصميمه لهذا الغرض والأضرار التي تقوم بها هذه البرامج قد تكون خفيفة كتغير اسم المؤلف لمستند ما أو كبيرة مثل الوصول الكامل للحاسوب دون المقدرة على تعقبها.

فيروسات الحاسب الآلي

فيروسات الكمبيوتر هي برامج تقوم بمهاجمة وإتلاف برامج معينة، وتنتقل الى برامج أخرى عند تشغيل البرامج المصابة.

ديدان الحاسوب

ديدان الحاسوب هي الفيروسات التي تقوم بإنشاء نسخ من تلقاء نفسها، يمكن أن تسبب الضرر بشكل واسع، على عكس الفيروسات، التي تتطلب نشر ملفات المضيف المصابة الديدان تعتبر برنامج مستقل ولا يحتاج إلى برنامج مضيف أو مساعدة أشخاص للنشر.

حصان طروادة

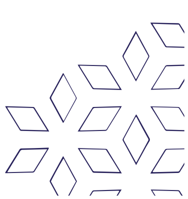
وهو من البرمجيات الخبيثة التي تبدو أنها برمجيات سليمة، تقوم بخداع المستخدمين من

أجل تحميلها وتطبيقها على أنظمتهم يتم تنشيطها، وتبدأ بمهاجمة النظام، فتؤدي إلى بعض الأمور المزعجة للمستخدم أو بعض الأضرار

برامج التجسس

هي مماثلة لبرامج الإعلانات، ولكن لديها نوايا ضارة، في حالة التجسس، المستخدم يجهل

هذا الغزو، ممكن لبرامج التجسس جمع ونقل المعلومات الشخصية، بسبب ما تقوم به هذه البرامج من نقل للمعلومات دون علم المستخدم، تصنف هذه البرامج على أنها برمجيات مقتحمة للخصوصية.



❖ أمن أنظمة التشغيل

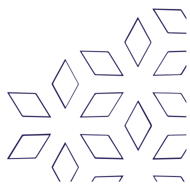
المقصود بأنظمة حماية نظم التشغيل

أول ما يتبادر للذهن عند الحديث عن أمان أنظمة التشغيل هو "أي نظام من أنظمة التشغيل يعتبر الأفضل من ناحية الأمان" سنحاول في هذه المقالة الإجابة عن هذا التساؤل محاولين الإحاطة بمختلف الجوانب التي يجب أخذها بعين الاعتبار عند البحث عن إجابة مفيدة.

تقدم أنظمة التشغيل مزايا أمان عديدة منها لحماية سرية البيانات أثناء التخزين والنقل والمعالجة، وأخرى لضمان أمانتها أي عدم إجراء تعديل غير مرغوب به عليها أثناء تخزينها ونقلها ومعالجتها وأيضا لضمان توافرها وعدم خسارتها بفعل خبيث أو بشكل غير مقصود، كما تقدم أنظمة التشغيل إمكانية إدارة التحكم بالوصول إلى الموارد Access Control وغيرها من ميزات الأمان التي تختلف بين نظام تشغيل وآخر.

إذا عند اختيار نظام التشغيل يجب معرفة ميزات الأمان التي يقدمها كل نظام تشغيل ومقارنتها مع ميزات الأمان في أنظمة التشغيل الأخرى لتكون هذه المعلومة عاملا إضافياً يجب أخذه بعين الاعتبار عند اختيار نظام التشغيل المناسب.

تستهدف أغلب التطبيقات الخبيثة نظام التشغيل نفسه، إذ أن ذلك يخولها اخفاء تواجدها عن المستخدم وبقية التطبيقات بما في ذلك برامج مضادات الفيروسات Antivirus Software ومضادات التطبيقات الخبيثة بشكل عام Antimalware والتي تتموضع في طبقة التطبيقات، ويخولها الوصول إلى العتاد مباشرة بما في ذلك القرص الصلب والشبكة ولوحة المفاتيح.. الخ دون معرفة المستخدم أو بقية التطبيقات، وهذا يعني بدوره أن المخترقين يحاولون البحث عن ثغرات أمنية موجودة في أنظمة التشغيل لتقوم برمجياتهم الخبيثة باستغلالها، وهي عملية شاقة تحتاج الكثير من الخبرة والكثير من الصبر وساعات عمل كثيرة، لذلك وبشكل بديهي يمكن استنتاج أن أغلب المخترقين يختارون البحث عن الثغرات في أنظمة التشغيل الأكثر شيوعا، لكي يكون مردود اكتشافهم لثغرة أمنية يمكن لبرامجهم الخبيثة استغلالها عاليا.



بالتالي، يمكن القول إنه كلما كان نظام التشغيل أكثر شيوعا كلما كان أكثر عرضة للاستهداف من قبل المخترقين وبالتالي أكثر عرضة لاكتشاف واستغلال ثغرات أمنية فيه، وبالتالي يحمل استخدامه بشكل عام خطورة أعلى من استخدام نظام تشغيل أقل انتشارا أو نظام تشغيل مبهم.

وبالتالي عند تقدير مستوى أمان نظام تشغيل ما، لا يكفي استخدام معايير مزايا الأمان التي يقدمها وإنما ينبغي أيضا بالإضافة لذلك مراجعة مستوى انتشاره وشيوعه في العالم.

اختراق أنظمة التشغيل - مزايا الأمان في أنظمة التشغيل

إدارة حسابات المستخدمين

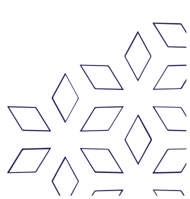
وتعني أن نظام التشغيل يتيح إمكانية إنشاء عدد من حسابات المستخدمين على الحاسب، وأن نظام التشغيل يتيح التحكم بالوصول Access Control كل من هذه الحسابات.

تحديثات الأمانSecurity Updates

تقوم الشركات التي تصدر نسخ أنظمة التشغيل بإصدار تحديثات الأمان بشكل دوري أو طارئ، لسد الثغرات الأمنية ولتحسين أداء واستقرار نظام التشغيل.

حالة الدعم التقني

تقوم الجهة المصدرة لنظام التشغيل بتقديم الدعم التقني لنظام التشغيل الذي يتضمن إصدار التحديثات، لسد الثغرات الأمنية بعد اكتشافها، عادة ما تقوم الجهة المصدرة لنظام التشغيل بتقديم الدعم هذا لعدد محدد من السنوات يتوقف بعدها الدعم ويتوقف معه إصدار تحديثات الأمان، وبالتالي تعد أنظمة التشغيل التي وصلت لنهاية عمرها الافتراضي end of life أنظمة تشغيل غير آمنة، ويتوجب على مستخدميها الانتقال لنظام تشغيل مازال مدعوما من الجهة المصدرة.

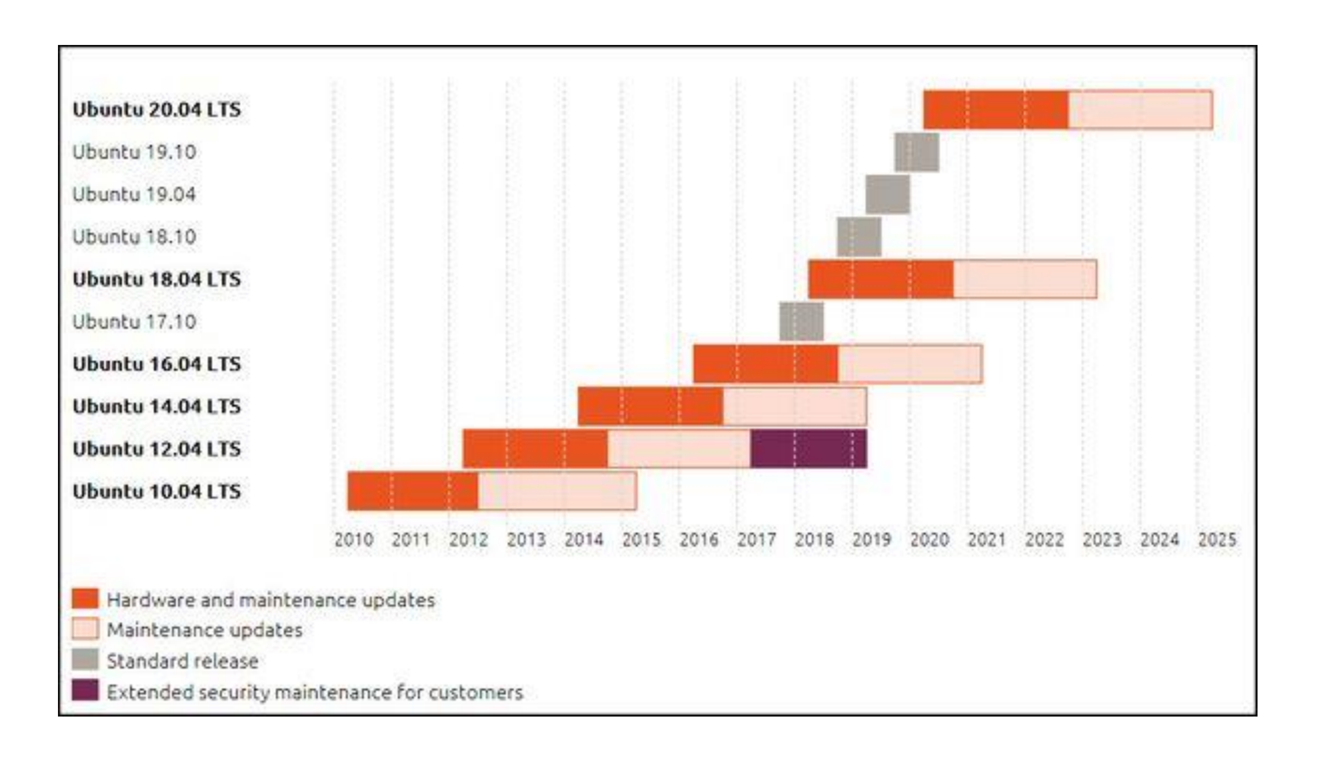


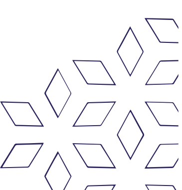
تختلف أنظمة التشغيل بعضها عن بعض بالنسبة للدعم التقني في عدة نقاط منها:

- مدة الدعم التقني أي عمر نظام التشغيل
- سرعة إصدار التحديثات الأمنية بعد اكتشاف الثغرات
- مصداقية الجهة المصدرة ودرجة تحملها للمسؤولية

على سبيل المثال، وصل Windows XP إلى نهاية عمره في ٨ نيسان/أبريل ٢٠١٤ بينما انتهى عمر نظام التشغيل Windows Vista في ١١ نيسان/أبريل ٢٠١٧ ومن المقرر أن يستمر دعم Windows 7 حتى ١٤ كانون الثاني/يناير ٢٠٢٠ و Windows 10 حتى ١٤ تشرين الأول/أوكتوبر ٢٠٢٥ ، للمزيد حول اصدارات نظام التشغيل Windows يمكن مراجعة الصفحة التالية Windows lifecycle fact sheet

كمثال آخر، يوضح الشكل التالي حالة الدعم التقني لنسخ المختلفة لنظام التشغيل أوبونتو Ubuntu



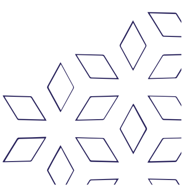


سلة المهملات

وهي مجلد يحتفظ بالملفات التي يقوم المستخدمون بحذفها إلى حين افراغها. إذا هي ميزة تتيح للمستخدم استعادة ملف تم حذفه سابقا طالما كان الملف موجودا في سلة المهملات. وهذا يعني أن احتمال فقدان ملف بسبب حذفه بالخطأ يصبح صغيرا. بنفس الوقت يعني ذلك أن على المستخدم الذي يريد فعلا حذف الملف، أن يقوم بعد حذفه بافراغ سلة المهملات، حذف الملفات بهذا الشكل غير كافي لتدميرها نهائيا من القرص الصلب، لذلك تتيح بعض أنظمة التشغيل إمكانية تدمير الملفات عند حذفها من سلة المهملات مثل نظام التشغيل Mac OS X بينما لا يتوجب استخدام تطبيقات إضافية للقيام بذلك على أنظمة تشغيل مثل Windows .

النسخ الاحتياطي

يعتبر إجراء النسخ الاحتياطية Backups للبيانات من أفضل الطرق لضمان عدم ضياع البيانات، توفر أنظمة التشغيل عادة ميزة إجراء النسخ الاحتياطي للبيانات على الجهاز أو لجزء منها كما تقدم إمكانية اجراء نسخة احتياطية لحالة نظام التشغيل بما في ذلك التطبيقات المنصبة على نظام التشغيل والتخصيصات التي قام المستخدم بتحديدها، ويتيح بعضها إمكانية حفظ النسخ الاحتياطية على السحابة مثل iCloud على نظام التشغيل ماك أو إس إكس Mac OS X ، و OneDrive على نظام التشغيل Windows .



مضاد الفيروساتAntivirus

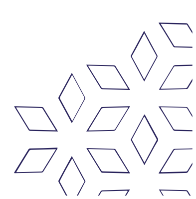
قد تتضمن نسخة نظام التشغيل برنامج مضاد للفيروسات Antivirus تنتجه وتدعمه الشركة التي تصدر نظام التشغيل وتبقي قاعدة بياناته محدثة بشكل مستمر، مثلا تتضمن نسخ نظام التشغيل Windows الحديثة مضاد الفيروسات والبرمجيات الخبيثة ويندوز ديفيندر Windows Defender في حين لا تتضمن الكثير من أنظمة التشغيل على مضاد فيروسات تتيح انظمة التشغيل المجال للشركات المختصة بمضادات الفيروسات والبرمجيات الخبيثة لاصدار نسخ متوافقة مع أنظمة التشغيل هذه وقادرة على حمايته.

جدار النار Firewall

ويقصد هنا جدار الحماية Firewall التي تعد جزءا من نظام التشغيل، يقوم جدار النار بحماية الجهاز المتصل بشبكة حواسيب من الاختراق أو التخريب أو تعطيل الخدمة عبر شبكة الحواسيب، مثلا يتضمن نظام التشغيل linux برنامج iptables الذي يمكن استخدامه لكي يقوم بمنع أي اتصال غير مرغوب به من جهاز آخر على الشبكة، لمزيد حول جدران النار هنا.

تشفير قرص نظام التشغيل

يعد تشفير القرص الصلب الطريقة الأفضل للابقاء على البيانات الموجودة على القرص الصلب سرية في حال ضياع الحاسب أو تعرضه للسرقة، فلو كان القرص الصلب غير مشفرا، يمكن للسارق معاينة محتويات القرص بدون الحاجة لكلمة سرّ نظام التشغيل على الجهاز وذلك عبر ربط القرص الصلب (فيزيائيا) بحاسب آخر يملكه السارق. يدعم عدد من أنظمة التشغيل ميزة تشفير قرص نظام التشغيل Operating System Disk Encryption نفسه بدون الحاجة لبرامج إضافية مثل نظام التشغيل وماك أو إس إكس Mac OS X ونظام التشغيل أوبونتو Ubuntu ، وانظمة آي أو إس iOS وأندرويد Android ونسخ Pro و Enterprise من نظام التشغيل ويندوز Windows في حين لا تقوم أنظمة تشغيل أخرى بتقديم هذه الميزة مثل نسخة Home من نظام التشغيل ويندوز Windows .

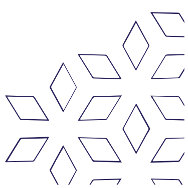


الخصوصيةPrivacy

تختلف أنظمة التشغيل فيما بينها بمستوى الخصوصية التي تؤمنه للمستخدم، فالكثير من أنظمة التشغيل تقوم مثلا بشكل دوري بإرسال سجلات الاستخدام إلى الجهة المصنعة لنظام التشغيل بهدف توفير معلومات تساعد على تحسين الخدمة، طبعا يترافق ذلك مع انخفاض مستوى خصوصية المستخدم إذ أن في ذلك كشفا للكثير من عادات المستخدم وطبيعة عمله وطبيعة استخدامه لنظام التشغيل، كما أن العديد من أنظمة التشغيل تتصل أوتوماتيكيا بالانترنت مستفسرة عن حالة الطقس، وعن أسعار العملات وعن العروض السينمائية والمسرحية في المكان الجغرافي المجاور، وعن عروض أسعار المنتجات والإعلانات لتعرضها للمستخدم.

مع ارتفاع اهتمام المستخدمين بالخصوصية، بدأ مصنعوا أنظمة التشغيل بتوفير إمكانية تغيير إعدادات الخصوصية لتناسب رغبة المستخدمين والتجاري القوانين والأنظمة السارية في الدول والمتعلقة بالخصوصية، فمثلا تقوم أنظمة التشغيل في يومنا هذا بسؤال المستخدم عن رغبته بإرسال بيانات الاستخدام إلى الجهة المصنعة، في حين لا تقوم أنظمة تشغيل أخرى بطلب إرسال بيانات استخدام معينة إلا عند حصول خطأ ما في نظام التشغيل أو في تطبيق ما.

مع التسريبات حول استغلال الحكومات وأجهزة الاستخبارات العلاقات أو النظام القضائي في دول كثير للتنصت ومراقبة المستخدمين، قام العديد من المطورين المهتمين بالخصوصية والأمن الرقمي بالعمل على إصدارة خاصة من إصدارات نظام التشغيل لينكس Linux أطلقوا عليها اسم تيلز Tails لتكون نسخة معدة للحفاظ على خصوصية المستخدم.

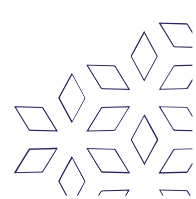


سجلات نظام التشغيلSystem Logs

تقوم أنظمة التشغيل عادة بالاحتفاظ بسجل أو أكثر يقوم نظام التشغيل بتدوين بيانات تتعلق بحالة وعمل نظام التشغيل مثل تسجيل الدخول وتسجيل الخروج، الأخطاء التي تطرأ خلال تشغيل البرامج، حالة الاتصال بالشبكة، وغيرها من المعلومات، كما تقوم العديد من الخدمات، وهي برامج تعد جزءا من نظام التشغيل، بتدوين بيانات متعلقة بحالتها وبعملها أيضا ضمن السجلات.

تختلف أنظمة التشغيل بكمية البيانات ونوعية البيانات التي تدون في السجلات وتختلف فيما بالإمكانيات التي تمنحها لمدير النظام لتحديد كمية المعلومات، فترة الاحتفاظ بها وإمكانية تعديلها.

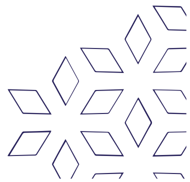
في حال استطاع أحدهم اختراق نظام التشغيل، سيرغب المخترق بإخفاء آثار الاختراق التي قد تكون مدونة في السجلات، كتسجيل. لذلك تختلف أنظمة التشغيل فيما بينها بمدى أمانة سجلاتها أي مدى مناعتها من التعديل أو الحذف.



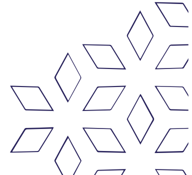
❖ مقارنة بين أنظمة التشغيل من حيث الأمان

يقدم الجدول التالي مقارنة نوعية بين أنظمة التشغيل من ناحية أمن المعلومات:

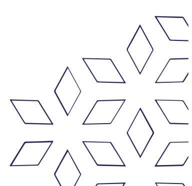
نظام التشغيل	نسبة الانتشار	إدارة حسابات المستخدمين	تنصيب التحديثات بشكل تلقائي	الدعم التقني	جدار النار	مضاد الفيروسات	تشفير قرص نظام التشغيل	سجلات نظام التشغيل
Windows XP Home	منخفضة	متوفر	الوضع الافتراضي: غير مفعل	حتى ٨ نيسان/أبريل ٢٠١٤	برامج من طرف ثالث	برامج من طرف ثالث	غير متوفر	
Windows 7 Home	مرتفعة	متوفر	الوضع الافتراضي: غير مفعل	حتى ١٤ كانون الثاني/يناير ٢٠٢٠	Windows Firewall: الوضع الافتراضي: غير مفعل , وبرامج من طرف ثالث	برامج من طرف ثالث	غير متوفر	متوفرة
Windows 7 Pro	منخفضة	متوفر	الوضع الافتراضي: غير مفعل	حتى ١٤ كانون الثاني/يناير ٢٠٢٠	Windows Firewall: الوضع الافتراضي: غير مفعل . وبرامج من طرف ثالث	Microsoft Defender وبرامج من طرف ثالث	متوفر، غير مفعل	متوفرة
Windows 10 Home	مرتفعة جدا	متوفر	الوضع الافتراضي: مفعل	حتى ١٤ تشرين	Windows Firewall: الوضع	Microsoft Defender	غير متوفر	متوفرة



				الأول/أوكتوبر ٢٠٢٥	الافتراضي: مفعل. وبرامج من طرف ثالث	وبرامج من طرف ثالث		
Windows 10 Pro	مرتفعة	متوفر	الوضع الافتراضي: مفعل	حتى ١٤ تشرين الأول/أوكتوبر ٢٠٢٥	Windows Firewall: الوضع الافتراضي: مفعل. وبرامج من طرف ثالث	Microsoft Defender وبرامج من طرف ثالث	متوفر، غير مفعل	متوفرة
Mac OS X 10.12 Sierra	منخفضة	متوفر	الوضع الافتراضي: غير مفعل	حتى ١ كانون الثاني/يناير ٢٠١٩	Application Firewall: الوضع الافتراضي: غير مفعل	برامج من طرف ثالث	متوفر، غير مفعل	متوفرة
Mac OS X 10.13 High Sierra	منخفضة	متوفر	الوضع الافتراضي: غير مفعل	حتى ١ تشرين الأول/أوكتوبر ٢٠٢٠	Application Firewall: الوضع الافتراضي: غير مفعل. وبرامج من طرف ثالث	برامج من طرف ثالث	متوفر، غير مفعل	متوفرة
Mac OS X 10.14 Mojave	منخفضة	متوفر	الوضع الافتراضي: غير مفعل	حتى ١ تشرين الأول/أوكتوبر ٢٠٢١	Application Firewall: الوضع الافتراضي:	برامج من طرف ثالث	متوفر، غير مفعل	متوفرة



					غير مفعل. وبرامج من طرف ثالث			
Mac OS X 10.15 Catalina	منخفضة	متوفر	الوضع الافتراضي: غير مفعل	الدعم مستمر، لا معلومات عن تاريخ إيقاف الدعم	Application Firewall: الوضع الافتراضي: غير مفعل. وبرامج من طرف ثالث	برامج من طرف ثالث	متوفر، غير مفعل	متوفرة
Ubuntu 14.04 LTS	منخفضة جدا	متوفر	الوضع الافتراضي: مفعل	حتى نيسان/أبريل ٢٠١٩	giptables الوضعufw الافتراضي غير مفعل	برامج من طرف ثالث	متوفر، خيار عند التنصيب	متوفرة
Ubuntu 16.04 LTS	منخفضة جدا	متوفر	الوضع الافتراضي: مفعل	نيسان/أبريل ٢٠٢١	giptables الوضعufw الافتراضي غير مفعل	برامج من طرف ثالث	متوفر، خيار عند التنصيب	متوفرة
Ubuntu 18.04 LTS	منخفضة جدا	متوفر	الوضع الافتراضي: مفعل	نيسان/أبريل ٢٠٢٣	giptables الوضعufw الافتراضي غير مفعل	برامج من طرف ثالث	متوفر، خيار عند التنصيب	متوفرة



❖ أنظمة حماية قواعد البيانات

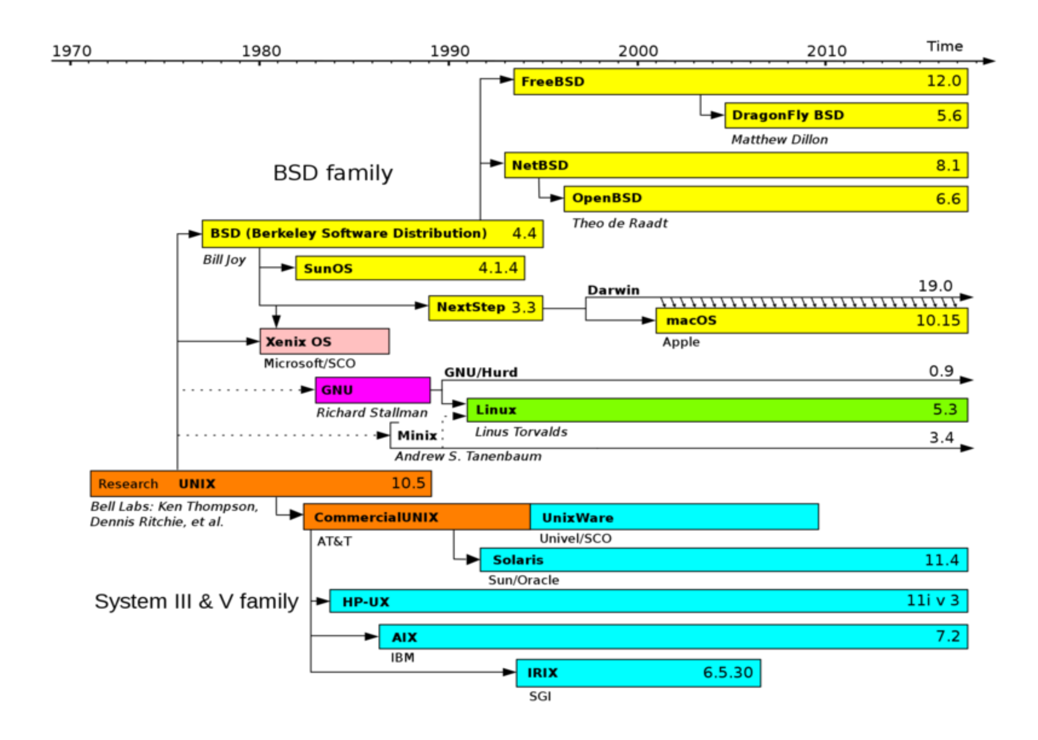
تصـنـف أنظمة التشـغيل ضـمـن عائلات كبيرة، تشـترك أنظمة التشـغيل في كـل عائلة منها بأصـل أو سلف مشترك، أكبر هذه العائلات، عائلة أنظمة تشغيل Unix التي تضـم نظام التشغيل Mac OS X ضـمـن أبنائها وعائلة أنظمة التشـغيل Linux التي تضـم كـلا مـن Ubuntu و Android ضـمـن أفرادها وعائلة أنظمة التشغيل Windows .

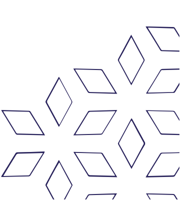
<u>عائلة أنظمة تشغيل Unix</u>

يمكن اعتبار نظام التشـغيل يونيكس Unix من أنظمة التشـغيل الأولى والتي تطورت مع تطور تقنية المعلومات وتغير مفاهيمها وتغير ظروف الســوق وحـاجـات المســتخـدمين، نشــأ نظام التشــغيل يونيكس Unix في الجامعات ومراكز الأبحاث مثل جامعة بيركلي Berkeley في كـاليفورنيا في الولايات المتحدة الأمريكية والتي مازال العديد من اصدارات نظام التشغيل Unix يحمل اسمها كما في أنظمة التشــغيل FreeBSD أوNetBSD، حيث يشــير الحرف B في BSD إلى الحرف الأول من اسم الجامعة.

يعد نظام التشـغيل ماك أو إس إكس Mac OS X الخاص بأجهزة Apple المختلفة من أكثر أنظمة التشغيل التي تنتمي إلى عائلة نظام التشغيل يونيكس Unix انتشارا وشهرة في يومنا هذا.

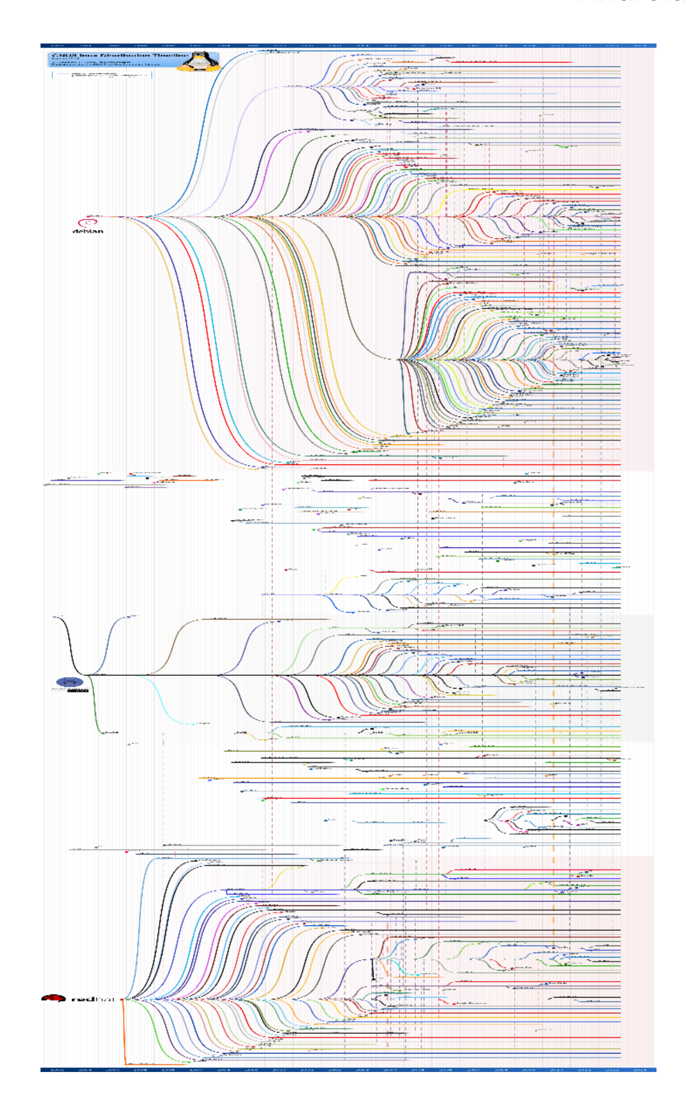
يبين المخطط التالي شجرة عائلة نظام التشغيل يونيكس.

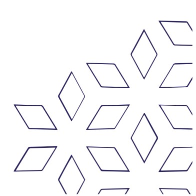




عائلة أنظمة تشغيل Linux

تعتد عائلة لينوكس Linux من أنظمة التشغيل العائلة الأكثر تنوعا، يوضح الشكل التالي تاريخ عائلة نظام التشغيل لينكس والإصدارات المختلفة له، من معاينة الشكل عن قرب، يمكن تحديد عدد من الفروع الهامة في شجرة العائلة مثل فروعDebian :، Slackwareو RedHat وجميعا "توزيعات" مختلفة من نظام التشغيل لينوكس، نلاحظ أن الشكل لا يتضمن نظام التشغيل أندرويد والسبب هو أن هناك الكثير من النقاش حول إذا كان نظام التشغيل أندرويد يعد جزءا من عائلة أنظمة التشغيل لينوكس أم لا، فنظام التشغيل Android يستخدم نواة لينوكس Linux Kernel وهي مجموعة من البرمجيات الأساسية ضمن نظام التشغيل لينوكس، لكنه العلاقة بين Android و Linux تقف عند هذا الحد، الذي لا يكفي بنظر الكثيرين لاعتبار Android جزءا من عائلة أنظمة التشغيل Android .

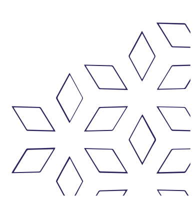




عائلة أنظمة تشغيل Windows

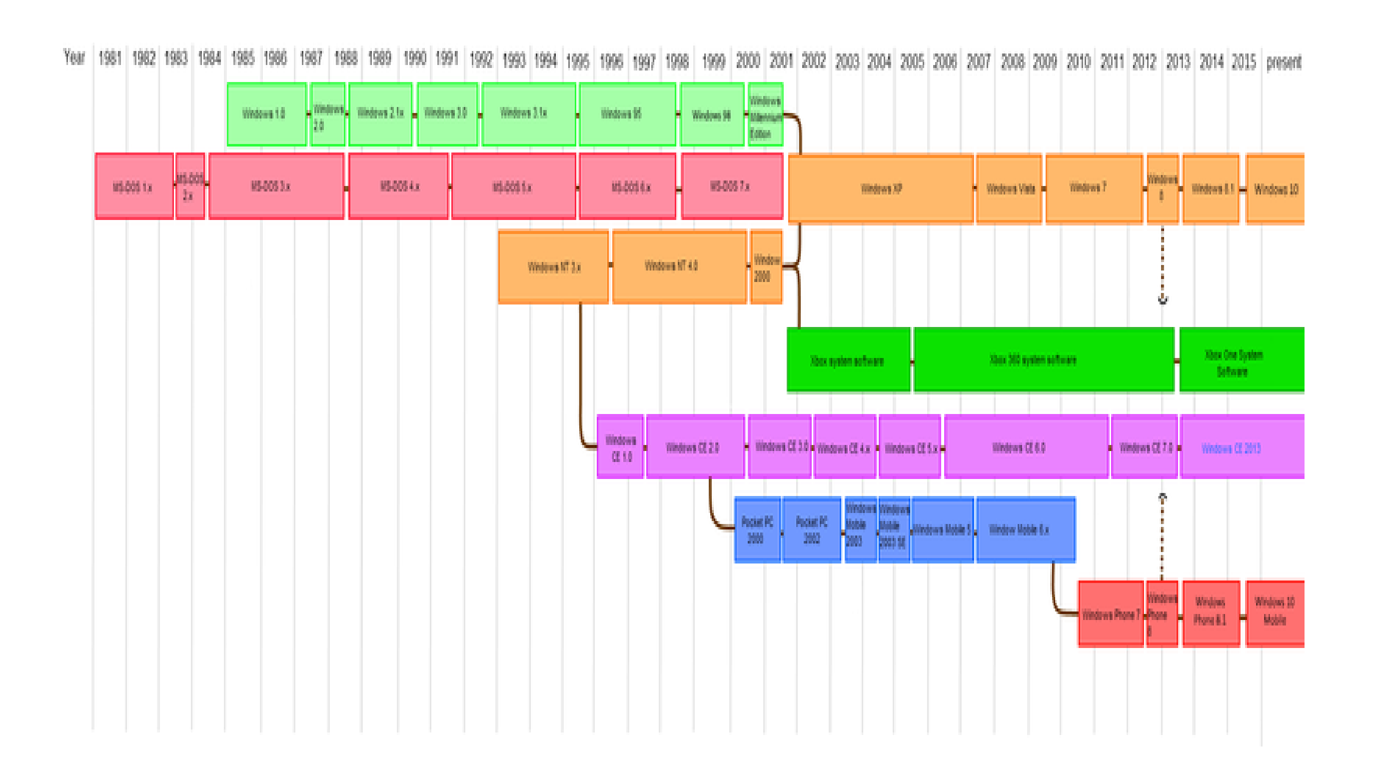
سبق نظام التشغيل ويندوز Windows نظام تشغيل آخر من شركة Microsoft سمي بنظام إدارة الأقراص من مايكروسوفت Microsoft Disk Operating System والذي عرف اختصارا بـــ إم إس دوسMS-DOS ، أو دوس DOS صدرت النسخة الأولى من MS-DOS عام ١٩٨١، وتبعها MS-DOS 2.0 منصف ١٩٨٣، وفي منتصف عام ١٩٨٤ وصل نظام التشغيل MS-DOS 3.0 إلى الأسواق، وفي ٢٠ تشرين الثاني/نوفمبر عام ١٩٨٥ صدرت النسخة الأولى من برنامج ويندوز Windows من قبل شركة مايكروسوفت Microsoft كواجهة تحكم صورية لنظام التشغيل إم إس–دوس MS-DOS 3.0. أي أن ويندوز لم يكن بذاته نظام التشغيل لكنه كان تطبيقاً ضمن نظام التشغيل إم إس دوس MS-DOS استمر اصدار نظام التشغيل MS-DOS حتى نهاية عام ٢٠٠٠ ومعه اصدارات مختلفة من برنامج Windows مثل الاصدارات Windows 2 و Windows 3 ثم Windows 95 الذي حصل على انتشار واسع جدا وكان آخرها Windows Millenium عام ٢٠٠٠.

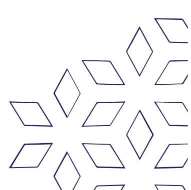
بالتوازي مع ذلك، قامت شركة مايكروسوفت بإصدار نظام تشغيل آخر أسمته ويندوز إن تي ٣,١ Windows NT عام ١٩٩٣ واستمرت بإصدار نصخ جديدة هي Windows NT 4.0 وآخرها Windows 2000.



عام ٢٠٠٠ قررت مايكروسوفت التوقف عن استخدام نظام التشغيل MS-DOS الذي تقادم عهده والاعتماد بشكل كامل على نظام التشغيل Windows NT الذي كان مواكبا لانتشار شبكات الحواسيب وعصر الانترنت، واصدرت نظام التشغيل ويندوز إكس بي Windows XP الذي تربع على عرش أكثر انظمة التشغيل انتشارا لسنوات عديد، أنظمة التشغيل Windows 7.0 و Windows 8.1 و Windows 10 هي أنظمة التشغيل التي مازالت شركة مايكروسوفت تدعمها وتوفر تحديثات الأمان لها.

ستصدر شركة مايكروسوفت نظام تشغيل خاص بالأنظمة المدمجة كالهواتف وأجهزة تحديد المواقع عبر الأقمار الصناعية يسمى ويندوز سي إي Windows CE وكذلك نظام تشغيل لمنصة الألعاب Xbox .



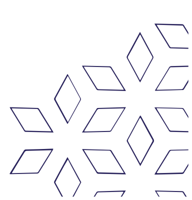


❖ المخاطر الأمنية لنظم قواعد البيانات

يتعلق أمن قاعدة البيانات باستخدام مجموعة واسعة من ضوابط أمن المعلومات لحماية قواعد البيانات (من المحتمل أن تشمل البيانات، وتطبيقات قواعد البيانات أو الوظائف المخزنة، وأنظمة قواعد البيانات، وخوادم قواعد البيانات، وروابط الشبكة المرتبطة) ضد التنازلات عن سريتها وسلامتها و التوفر، وهي تتضمن أنواعاً أو فئات مختلفة من الضوابط، مثل التقنية والإجرائية / الإدارية والمادية.

تشمل مخاطر الأمان على أنظمة قواعد البيانات، على سبيل المثال:

- نشاط غير مصرح به أو غير مقصود أو إساءة استخدام من قبل مستخدمي قاعدة البيانات المصرح لهم، أو مسؤولي قاعدة البيانات، أو مديري الشبكة / الأنظمة، أو من قبل المستخدمين أو المتسللين غير المصرح لهم (مثل الوصول غير المناسب إلى البيانات الحساسة أو البيانات الوصفية أو الوظائف داخل قواعد البيانات، أو التغييرات غير الملائمة لبرامج قواعد البيانات أو الهياكل أو التكوينات الأمنية).
- الإصابات بالبرامج الضارة التي تسبب حوادث مثل الوصول غير المصرح به، أو تسرب أو الكشف عن البيانات الشخصية، أو الخاصة، أو حذف البيانات، أو البرامج أو إتلافها، أو انقطاع أو رفض الوصول المصرح به إلى قاعدة البيانات، والهجمات على الأنظمة الأخرى، والفشل غير المتوقع لخدمات قاعدة البيانات.
- الأحمال الزائدة وقيود الأداء وقضايا السعة التي تؤدي إلى عدم قدرة المستخدمين المصرح لهم على استخدام قواعد البيانات على النحو المنشود.
- الأضرار المادية لخوادم قاعدة البيانات الناتجة عن حرائق غرفة الكمبيوتر أو الفيضانات، والسخونة الزائدة، والبرق، وانسكاب السوائل العرضي، والتفريغ الساكن، والأعطال الإلكترونية / أعطال المعدات وتقادمها.

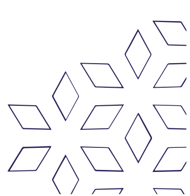


- عيوب التصميم وأخطاء البرمجة في قواعد البيانات والبرامج والأنظمة المرتبطة بها، مما يؤدي إلى ظهور العديد من نقاط الضعف الأمنية (مثل تصعيد الامتيازات غير المصرح به) وفقدان / تلف البيانات وتدهور الأداء وما إلى ذلك.
- تلف و / أو فقدان البيانات الناتج عن إدخال بيانات أو أوامر غير صالحة، وأخطاء في قاعدة البيانات أو عمليات إدارة النظام، والتخريب / الضرر الجنائي وما إلى ذلك.

كثيرًا ما قال روس ج. أندرسون إن قواعد البيانات الكبيرة بطبيعتها لن تكون أبداً خالية من إساءة الاستخدام من خلال انتهاكات الأمن؛ إذا تم تصميم نظام كبير لتسهيل الوصول إليه، فإنه يصبح غير آمن؛ إذا كان مانعاً للماء يصبح من المستحيل استخدامه، ُعرف هذا أحياناً باسم قاعدة أندرسون.

❖ جدران الحماية وأنواعها

تاريخياً مصطلح"Firewall"يعود إلى أكثر من قرن؛ حيث أن العديد من البيوت قد تم بنائها من طوب في الحائط بشكل يوقف انتقال النيران المحتملة، هذالحائط الطوبي يسمي بالـــ"حائط الناري"، وفي أواخر الثمانينات ظهرت تقنية الجدار الناري عندما كان الإنترنت تقنية جديدة نوعًا ما من حيث الاستخدام العالمي، فالفكرة الأساسية ظهرت استجابة لعدد من الاختراقات الأمنية الرئيسية لشبكة الإنترنت التي حدثت في أواخر الثمانينات، فاصبحت جدران الحماية خط الدفاع الأول في الأمان الشبكي، فهي تنشئ حاجزاً "جهاز أو برنامج "بين الشبكات الداخلية الآمنة والمسيطر عليها وبين الشبكات الخارجية غير الموثوق بها، مثل الإنترنت، فيرفض أو يسمح بمرور بيانات او برنامج وفقاً لقواعد معينة، فمن دون الإعداد الملائم فإنه غالباً ما يصبح الجدار الناري عديم الفائدة، ومن ثم بعدها بدات الاجيال والتعديلات لهذه التقنية.

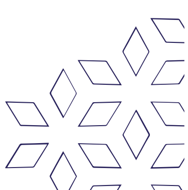


فما هي هذه الاجيال من جدران الحماية؟

<u>الجيل الأول: مرشحات الحزمة(Packet Filters)</u>

أول بحث نشر عن تقنية الجدار الناري كان عام ١٩٨٨، عندما قام مهندسون من(DEC) بتطوير نظام مرشح عرف باسم جدار النار بنظام فلترة حزمة البيانات، هذا النظام الأساسي يمثل الجيل الأول الذي سوف يصبح عالي التطور في مستقبل أنظمة أمان الإنترنت، فكانت طريقة عملفلترة الحزمة كانت تقوم بالتحقق من حزم البيانات التي تمثل الوحدة الأساسية المخصصة لنقل البيانات بين الحواسيب على الإنترنت فإذا كانت الحزمة تطابق مجموعة شروطات المرشح فإن النظام سيسمح بمروها أو يرفضها (يتخلص منها ويقوم بإرسال إشارة "خطأ" للمصدر).

هذا النظام من المرشحات لا يعير اهتماما إلى كون حزمة البيانات جزءاً من تيار المعلومات، فلا يخزن معلومات عن حالة الاتصال، وبالمقابل فإنه كان يرشح الحزم بناءً على المعلومات المختزنة في حزمة البيانات نفسها(بمعنى انه يستخدم توليفة من مصدر الحزمة للجهة الذاهبة إليه، النظام المتبع، ورقم المرفأ المخصص لـ(UDP) (TCP) الذي يشمل معظم تواصل الإنترنت، لأن (TCP) و (UDP) في العادة تستخدم منافذ معروفة إلى أنواع معينة من قنوات المرور، فكانت هذه الفلترة "عديم الحالة" تميز وتتحكم بهذه الأنواع من القنوات (مثل تصفح المواقع، الطباعة البعيدة المدى، إرسال البريد الإلكتروني، إرسال الملفات)، إلا إذا كانت الأجهزة على جانبي فلتر الحزمة يستخدمان نفس المنافذ الغير اعتيادية.



الجيل الثاني: فلتر محدد الحالة (Stateful Filters)

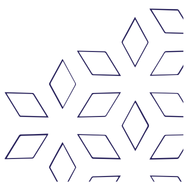
هنا يقوم جدار الحماية بمراقبة حقول معينة في الحزمة، ويقارنها بالحقول المناظرة لها في الأخرى التي في السياق نفسه، ونعني بالسياق هنا مجموعة المظاريف الإلكترونية المتبادلة عبر شبكة الإنترنت بين جهازين لتنفيذ عملية ما، وتجري غربلة المظاريف التي تنتمي لسياق معين إذا لم تلتزم بقواعده؛ لأن هذا دليل على أنها زرعت في السياق وليست جزءا منه، مما يثير الشكوك بأنها برامج مسيئة أو مظاريف أرسلها متطفل.

الجيل الثالث: طبقات التطبيقات (Application Layer Firewall)

الفائدة الرئيسية من الجدار الناري لطبقات التطبيقات أنه يمكن أن "يفهم" بعض التطبيقات والأنظمة مثل نظام نقل الملفات"DNS"تصفح المواقع، أيضاً يمكنه أن يكتشف إذا ما كان هنالك نظام غير مرغوب فيه يتم تسريبه عبر منافذ غير اعتيادية أو إذا كان هنالك نظام يتم إساءة استخدامه بطريقة مؤذية ومعروفة.

أنواع جدران الحماية

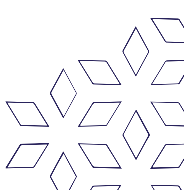
هنالك العديد من فئات الجدران النارية بناءً على مكان عمل الاتصال، ومكان تشفير الاتصال والحالة التي يتم تتبعها.



- **طبقات الشبكة ومفلترات الحزم (Network Layer and Packet Filters)**

الجدار الناري ذو طبقات الشبكة والذي يسمى أيضا مفلتر الحزم، يعمل على أنظمةTCP\IPمنخفضة المستوى، ولا يسمح للحزم بالمرور عبر الجدار الناري دون أن تطابق مجموعة القوانين المحددة، المحددة من المسؤول عن الجدار الناري وإن لم يتم هذا تطبق الأوامر الطبيعية، وهذا النوع ينقسم إلى قسمين فرعيين اثنين: ذو الحالة وعديم الحالة، تتحفظ الجدران النارية ذات الحالة بنطاق يتعلق بالجلسات المفتوحة حالياً، ويستخدم معلومات الحالة لتسريع معالجة الحزمة، أي اتصال شبكي يمكن تحديده بعدة امور، تشتمل على عنوان المصدر والوجهة، منافذ UDP وTCP، والمرحلة الحالية من عمر الاتصال (يشمل ابتداء الجلسة، المصافحة، نقل البيانات، وإنهاء الاتصال) وإذا كانت الحزمة لاتطابق الاتصال الحالي فسوف يتم تقدير ماهيتها طبقاً لمجموعة الأوامر للاتصال الجديد، وإذا كانت الحزمة تطابق الاتصال الحالي بناءً على مقارنة عن طريق جدول الحالات للحائط الناري، فسوف يسمح لها بالمرور دون معالجة أخرى، أما الجدار الناري العديم الحالة يحتوي على قدرات فلترة الحزمة،ولكن لا يستطيع اتخاذ قرارات معقدة تعتمد على المرحلة التي وصل لها الاتصال بين المضيفين.

"الجدران النارية الحديثة يمكنها ان تفلترالقنوات معتمدة على كثير من الجوانب للحزمة، مثل عنوان المصدر، منفذ المصدر، عنوان الوجهة ، نوع خدمة الوجهة مثل"WWW"و"FTP"، ويمكن أن يفلتر اعتماداً على أنظمة وقيم"TTL"، صندوق الشبكة للمصدر، اسم النطاق للمصدر، والعديد من الجوانب الأخرى".



- **طبقات التطبيقات(Application Layer)**

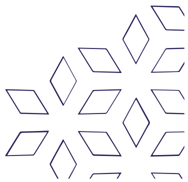
تعمل الجدران النارية لطبقات التطبيقات على مستوى التطبيق لقواعد"TCP\IP"مثل جميع أزمنة المتصفح، أو جميع أزمنة"TELNET"و"FTP"، ويمكن أن يعترض جميع الحزم المنتقلة من وإلى التطبيق فيمكأنه ان يحجب الحزم الأخرى دون إعلام المرسل عادة، وعند تحري الحزم جميعها لإيجاد محتوى غير ملائم، يمكن للجدار الناري أن يمنع الديدان (worms) والأحصنة الطروادية (Trojan horses) من الانتشار عبر الشبكة، ولكن عبر التجربة تبين أن هذا الأمر يصبح معقدا جداً ومن الصعب تحقيقه مع الأخذ بعين الاعتبار التنوع في التطبيقات وفي المضمون المرتبط بالحزم وهذا الجدار الناري الشامل لا يحاول الوصول إلى مثل هذه المقاربة.

- **خادم الوكيل(Proxy Servers)**

قد يعمل كجدار ناري بالاستجابة إلى الحزم الداخلة (طلبات الاتصال على سبيل المثال) بطريقة تشبه التطبيق مع المحافظة على حجب الحزم الأخرى، كما يجعل العبث بالأنظمة الداخلية من شبكة خارجية أصعب ويجعل إساءة استخدام الشبكة الداخلية لا يعني بالضرورة اختراق أمني متاح من خارج الجدار الناري طالما بقي تطبيق الخادم سليماً ومعداً بشكل ملائم، بالمقابل فإن المتسللين قد يختطفون نظاماً متاحاً للعامة ويستخدمونه كخادم وكيل لغاياتهم الشخصية، بحيث يستخدمون أساليب مثل"IP Spoofing"لمحاولة تمرير حزم بيانات إلى الشبكة المستهدفة.

- **ترجمة عنوان الشبكة(Network Address Translation)**

عادة ما تحتوي الجدران النارية على وظيفة ترجمة عنوان الشبكة (NAT)، ويكون المضيفين محميين خلف جدار ناري يحتوي على مواقع ذو نطاق خاص فتكون الجدران النارية متضمنة على هذه الميزة لتحمي الموقع الفعلي للمضيف المحمي، وبالأصل تم تطوير خاصية"NAT"لتخاطب مشكلة كمية"IPv4"المحدودة والتي يمكن استخدامها وتعيينها للشركات أو الأفراد وبالإضافة إلى تخفيض العدد وبالتالي كلفة إيجاد مواقع عامة كافية لكل جهاز في المنظمة، وأصبح إخفاء مواقع الإجهزة المحمية أمراً متزايد الأهمية للدفاع ضد استطلاع الشبكات.



❖ التهديدات الالكترونية الشائعة

من أنواع التهديدات الأمنية، مثلاً البرامج الضارة واستخراج البيانات وتسرُّب البيانات وخرق الحساب، للحصول على أوصاف لهذه التهديدات الأمنية، يُرجى الاطّلاع على الأقسام أدناه .

استخراج البيانات

يعتبر استخراج البيانات نسخ أو نقل غير مُصرَّح به للبيانات خارج نطاقك، قد يتم إجراء هذا النقل يدوياً بواسطة شخص يمكنه الوصول لموارد داخل مؤسستك، أو قد يكون النقل تلقائياً تنفذه برامج ضارة في شبكتك، على سبيل المثال، يمكن سرقة البيانات عن طريق خرق حساب يمتلك إمكانية الوصول إلى البيانات، أو من خلال تثبيت تطبيق طرف ثالث يُرسل البيانات خارج نطاقك.

تسرُّب البيانات

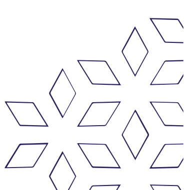
تسرُّب البيانات هو عملية نقل غير مصرّح بها لبيانات حساسة خارج نطاقك، يمكن حدوث تسرُّب البيانات عن طريق البريد الإلكتروني أو Google Meet أو Google Drive أو المجموعات أو أجهزة الجوَّال، قد تحدث التسريبات بسبب سلوك ضار أو غير ضار، مثلاً بسبب تفعيل الوصول للجميع إلى المجموعات أو من إعدادات المشاركة السهلة لخدمة Google Drive أو من أجهزة الجوَّال المُخترَقة أو من مرفقات البريد الإلكتروني الصادر.

حذف البيانات

حذف البيانات هو الحذف الضار للبيانات والذي ينتج عنه صعوبة استرداد البيانات أو استحالة استردادها، على سبيل المثال، قد ينفّذ مهاجم برنامج فدية يُشفّر بياناتك، ثم يطلب دفعة نقدية لمفتاح التشفير الذي يفك تشفير البيانات.

مستخدم داخلي ضار

المستخدم الداخلي الضار هو مستخدم موافق عليه أو مشرف في مؤسستك يُسرب معلومات حساسة بشكل خبيث خارج نطاقك، المستخدم الداخلي الضار قد يكون موظفاً، أو موظفاً سابقاً أو مقاولاً أو شريكاً، قد يُسرب المستخدم الداخلي الضار البيانات عبر أجهزة جوال مُختَرَقة أو عن طريق إرسال المحتوى خارج نطاقك عبر البريد الإلكتروني.



خرق الحساب

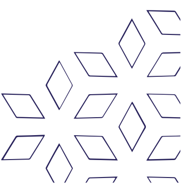
خرق الحساب هو وصول غير مُصرَّح به لحساب مستخدم أو مشرف داخل نطاقك، يحدث خرق الحساب بسبب سرقة مستخدم غير مفوَّض لبيانات اعتماد تسجيل الدخول، وبحسب هذا التصور، يتم اختراق الحساب في نطاقك بطريقة يُمكن أن يستخدمها مهاجم للتفاعل مع الموارد، إحدى الطرق الشائعة في سرقة بيانات الاعتماد هي التصيد الاحتيالي المُوجَّه عندما يُرسل المخترقون رسالة إلكترونية احتيالية تَبدو وكأنها واردة من فرد أو منشأة تجارية تعرفها وتثق بها.

تعلية الامتيازات

يشير تعلية الامتيازات إلى مهاجم تَمكن من اختراق حساب أو أكثر في نطاقك، ويعمل على الاستفادة من تلك الامتيازات المحدودة للحصول على إمكانية الدخول إلى حسابات ذات امتيازات أكبر. عادةً ما يحاول هذا النوع من المخترقين الوصول إلى امتيازات المشرف العام للحصول على تحكُّم أكبر في موارد نطاقك.

اختراق كلمة المرور

اختراق كلمة المرور هي عملية استرداد كلمات المرور باستخدام برنامج متخصّص وحوسبة ذات سعة عالية، يمكن للمهاجمين تجربة عدة مجموعات مختلفة لكلمة المرور خلال مدة زمنية قصيرة، من إحدى استراتيجيات منع خرق كلمة المرور، هي فرض التحقُّق بخطوتين للمستخدمين والمشرفين في نطاقك، كما تُغلق Google أيضاً أي حساب عند رصد نشاط مريب.



التصيُّد الاحتيالي/التصيُّد الاحتيالي للبيانات المهمة

التصيُّد الاحتيالي/التصيُّد الاحتيالي للبيانات المهمة هو ممارسة احتيالية تتم بإرسال رسائل إلكترونية تبدو أنها واردة من شركات معروفة لخداع الأفراد من أجل كشف معلومات شخصية، مثل كلمات المرور وأرقام الحسابات، أو للحصول على التحكُّم في حساب مستخدم في نطاقك، **هناك ثلاثة فروق في التصيُّد الاحتيالي:**

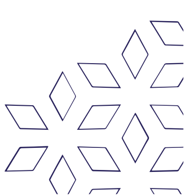
- هجوم التصيُّد الاحتيالي رسائل إلكترونية مستهدفة بشكل عام والتي تعمل من خلال أعداد كبيرة من الرسائل منخفضة التكلفة إلى العديد من المستخدمين، قد تتضمن الرسالة رابطًا لموقع إلكتروني يدعو المستخدمين إلى الاشتراك لربح جائزة نقدية، ومن خلال الاشتراك، تُعطي الضحية بيانات اعتماد تسجيل الدخول التابعة لها .
- هجوم التصيُّد الاحتيالي المستهدف هو هجوم يستهدف أفراداً بعينهم، مثلاً، حث محاسب على فتح مرفقات تُثبّت برامج ضارة، ثم تساعد البرامج الضارة المهاجم في الوصول إلى بيانات الحسابات والبنوك.
- هجوم التصيُّد الاحتيالي للبيانات الهامة هي محاولة خداع أفراد لأخذ إجراءات محددة مثل إجراء تحويل نقدي، يتم تصميم خدمة التصيُّد الاحتيالي للبيانات المهمة بحيث تتخفّى كرسالة إلكترونية مهمة تتعلّق بالنشاط التجاري، ومُرسلة من سلطة قانونية.

الانتحال

الانتحال هو تزييف رأس الرسالة الإلكترونية بواسطة مهاجم لكي تبدو الرسالة صادرة من شخص آخر غير المصدر الحقيقي، عندما يرى أحد المستخدمين مُرسِل الرسالة، قد يبدو له شخصاً يعرفه أو أنها صادرة من نطاق يثق به، انتحال البريد الإلكتروني هو تكتيك يُستخدم في التصيُّد الاحتيالي وحملات الرسائل غير المرغوب فيها بسبب أن مستخدمي البريد الإلكتروني غالباً ما يفتحون الرسالة إذا اعتقدوا أنها واردة من مصدر قانوني.

البرامج الضارة

البرامج الضارة هي برامج تم تصميمها لغرض ضار، مثل فيروسات الكمبيوتر وفيروسات حصان طروادة وبرامج التجسس والبرامج الضارة الأخرى.



خامساً: أمن الحاسوب والبرمجيات

في هذا الفصل سنتعرف على المواضيع التالية:

- أمن الحاسوب
- أمن الملفات
- التهديدات الرقمية للحاسبات والبرمجيات (عملي)
- أمن أنظمة التشغيل
- مقارنة بين أنظمة التشغيل من حيث الأمان
- أنظمة حماية قواعد البيانات
- المخاطر الأمنية لنظم قواعد البيانات
- جدران الحماية وأنواعها
- التهديدات الالكترونية الشائعة

❖ مفهوم أمن الشبكات

هندسة امن الشبكات والمعلومات هي ممارسة لمنع الدخول غير المصرح به إلى الشبكات والحماية منه، كفلسفة، فإنه يكمل أمان نقطة النهاية الذي يركز على الأجهزة الفردية، تركز هندسة امن الشبكات والمعلومات بدلاً من ذلك على كيفية تفاعل هذه الأجهزة وعلى النسيج الضام بينها.

يأخذ معهد SANS تعريف هندسة امن الشبكات والمعلومات إلى أبعد من ذلك:

هندسة امن الشبكات والمعلومات هي عملية اتخاذ تدابير وقائية مادية وبرمجية لحماية البنية التحتية للشبكات الأساسية من الوصول غير المصرح به أو سوء الاستخدام، أو الأعطال، أو التعديل، أو التدمير، أو الكشف غير المناسب، وبالتالي إنشاء نظام أساسي آمن لأجهزة الكمبيوتر والمستخدمين والبرامج لأداء المسموح لهم من وظائف حاسمة في بيئة آمنة.

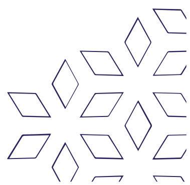
لكن الاتجاه العام هو نفسه: يتم تنفيذ هندسة امن الشبكات والمعلومات من خلال المهام والأدوات التي تستخدمها لمنع الأشخاص أو البرامج غير المصرح لهم من الوصول إلى شبكاتك والأجهزة المتصلة بها، في الأساس، لايمكن اختراق جهاز الكمبيوتر الخاص بك إذا لم يتمكن القراصنة من الوصول إليه عبر الشبكة.

أساسيات هندسة امن الشبكات والمعلومات

كيف تضع خطة لتنفيذ هذه الرؤية؟ كتب ستيفن نورثكوت كتاباً تمهيدياً عن أساسيات هندسة امن الشبكات والمعلومات ونشعر بقوة أن رؤيته للمراحل الثلاث لإزالة مهددات امن المعلومات والشبكات لا تزال ذات صلة ويجب أن تكون الإطار الأساسي لاستراتيجيتك، في روايته، **يتكون أمن الشبكة من:**

- الحماية من مهددات امن المعلومات والشبكات: يجب عليك تكوين أنظمتك وشبكاتك بشكل صحيح قدر الإمكان.
- الكشف: يجب أن تكون قادراً على تحديد متى تغير التكوين أو عندما تشير بعض حركة مرور الشبكة إلى وجود مشكلة.
- رد الفعل: بعد تحديد المشكلات بسرعة، يجب أن تستجيب لها وتعود إلى الحالة الآمنة بأسرع ما يمكن

هذا، باختصار، هو استراتيجية الدفاع في العمق، إذا كان هناك موضوع واحد مشترك بين خبراء الأمن، فهو أن الاعتماد على خط دفاع واحد أمر خطير، لأن أي أداة دفاعية واحدة يمكن هزيمتها من قبل خصم مصمم من مهددات امن المعلومات والشبكات. شبكتك ليست خطا أو نقطة: إنها منطقة، وحتى إذا قام أحد المهاجمين بغزو جزء منها، فلا يزال لديك الموارد لإعادة طردهم، إذا كنت قد نظمت دفاعك بشكل صحيح.



❖ أهداف الحماية الأمنية للشبكات(عملي)

سرية المعلومات

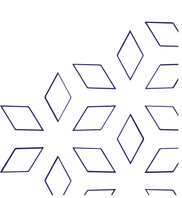
Data Confidentiality وهذا الجانب يشتمل على الإجراءات والتدابير اللازمة لمنع اطلاع غير المصرح لهم على المعلومات التي يطبق عليها بند السرية أو المعلومات الحساسة، وهذا هو المقصود بأمن وسرية المعلومات، وطبعاً درجة هذه السرية ونوع المعلومات يختلف من مكان لآخر وفق السياسة المتبعة في المكان نفسه، ومن أمثلة هذه المعلومات التي يجب سريتها المعلومات الشخصية للأفراد.

تكامل المعلومات

Data Integrity في هذا الجانب لا يكون الهم الأكبر هو الحفاظ على سرية المعلومات وإنما يكون الحفاظ على سلامة هذه المعلومات من التزوير والتغيير بعد إعلانها على الملأ، فقد تقوم هيئة ما بالإعلان عن معلومات مالية أو غيرها تخص الهيئة وهنا يأتي دور الحفاظ على السلامة بأن تكون هذه المعلومات محمية من التغيير أو التزوير، ومن أمثلة ذلك مثلاً: إعلان الوزارات أو الجامعات عن أسماء المقبولين للعمل بها، تتمثل حماية هذه القوائم في أن تكون مؤمنة ضد التغيير والتزوير فيها بحذف أسماء ووضع أسماء غيرها مما يسبب الحرج والمشكلات القانونية للمؤسسات، وأيضاً بالنسبة للمعلومات المالية بتغيير مبلغ مالي من ١٠٠ إلى ١٠٠٠٠٠ وهذا هام جداً لما يترتب عليه من خسائر فادحة في الأموال.

توافرية الشبكة

Availability لعله من المنطقي أن نعرف أن كل إجراءات وصناعة المعلومات في الأساس تهدف إلى هدف واحد وهو إيصال المعلومات والبيانات إلى الأشخاص المناسبين في الوقت المناسب، وبالتالي فإن الحفاظ على سرية المعلومات وضمان سلامتها وعدم التغيير فيها لايعني شيئاً إذا لم يستطع الأشخاص المخولين أو المصرح لهم الوصول إليها، وهنا تأتي أهمية الجانب الثالث من جوانب أو مكونات أمن المعلومات وهو ضمان وصول المعلومات إلى الأشخاص المصرح لهم بالوصول إليها من خلال توفير القنوات والوسائل الآمنة والسريعة للحصول على تلك المعلومات، وفي هذا الجانب يعمل المخربون بوسائل شتى لحرمان ومنع المستفيدين من الوصول إلى المعلومات مثل حذف المعلومات قبل الوصول إليها أو حتى مهاجمة أجهزة تخزين المعلومات وتدميرها أو على الأقل تخريبها.



❖ مفهوم الثغرات في أمن الشبكات

احياناً يتم نشـر تنبيه لثغرة منتشـرة في إحدى التطبيقات أو المواقع التي نسـتخدمها، وقد يدفعك الفضـول للتسـاؤل عما تكون هذه الثغرات، وكيف يتم إنشـاءها، وكيف يتم كشـفها وكيف يتم استغلالها، هذه المقالة ستتحدث عن مفهوم الثغرات الأمنية .

ماهي الثغرات الأمنية؟

هي نقطة ضـعف أو عيب أو خطأ يتم العثور عليه داخل النظام والذي يُمكن أن يتم الاسـتفادة منه من قبل المخترقين لاختراق شبكة آمنة.

كيف يتم إنشاء الثغرات الأمنية؟

الثغرات الأمنية هي عيب في كتابة أكواد البرنامج أو خطأ في تكوين النظام والسـبب البسـيط هو أن الثغرات الأمنية هي خاصـية ناشـئة للبرامج وهناك ثلاثة أسـباب رئيسـية: جودة الكود، والتعقيد، ومدخلات البيانات الموثوقة.

كيف يتم استغلال الثغرات الأمنية؟

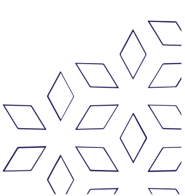
الاسـتغلال هو الخطوة التالية في دليل المخترق بعد اكتشـاف الثغرة الأمنية وهو جزء من برنامج أو نص برمجي يمكن أن يسمح للقراصنة بالسيطرة على النظام واستغلال نقاط الضعف فيه ويستخدم المخترقون عـادةً أدوات فحص الثغرات الأمنيـة مثـل Nessus و Nexpose و OpenVAS وغيرها للعثور على هذه الثغرات الأمنية.

كيف يمكن الكشف عن الثغرات الأمنية؟

عن طريق فحص الأمان لتطبيق باسـتخدام أدوات الطرف الثالث ومراقبة الثغرات الأمنية بانتظام في التطبيقات أو البيئات ذات الصلة واختبارات الإختراق .

اختبار الاختراق :

هو محاكاة هجوم إلكتروني ضد نظام الكمبيوتر لديك للتحقق من نقاط الضعف القابلة للاستغلال.



❖ التهديدات الرقمية لشبكات الحاسب

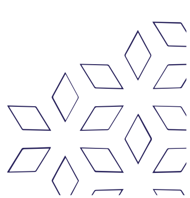
الاختراق

الاختراق الأمني هو أي حادث ينتج عنه وصول غير مصرح به إلى بيانات الكمبيوتر أو التطبيقات أو الشبكات أو الأجهزة، كما ينتج عنه الوصول إلى المعلومات دون إذن، ويحدث عادةً عندما يتمكن المتسلل من تجاوز آليات الأمان.

من الناحية الفنية، يوجد فرق بين الاختراق الأمني واختراق البيانات يُعد الاختراق الأمني بمثابة اختراق فعال، في حين يتم تعريف اختراق البيانات على خروج المجرم الإلكتروني بالمعلومات، تخيل اللص؛ حيث ينفّذ اختراقاً أمنياً عندما يتسلق النافذة، بينما ينفّذ اختراق بيانات عندما يلتقط محفظتك أو الكمبيوتر المحمول ويأخذه.

المعلومات السرية لها قيمة هائلة، وغالباً ما يتم بيعها على الإنترنت المظلم (دارك ويب)؛ على سبيل المثال، يمكن شراء الأسماء وأرقام بطاقات الائتمان، ثم استخدامها لأغراض سرقة الهوية أو الاحتيال، وليس من المستغرب أن الاختراقات الأمنية يمكن أن تكلف الشركات مبالغ ضخمة من المال، حيث يبلغ متوسط التكلفة حوالي ٤ ملايين دولار بالنسبة للشركات الكبرى.

ومن المهم أيضاً التمييز بين تعريف الاختراق الأمني وتعريف الحادث الأمني، فقد يتضمن الحادث إصابة بالبرامج الضارة أو هجوم DDOS أو ترك أحد الموظفين لكمبيوتر محمول في سيارة أجرة، ولكن إذا لم ينتج عنه وصول إلى الشبكة أو فقدان البيانات، فلن يتم اعتباره اختراقاً أمنياً.



أنواع الاختراقات الأمنية

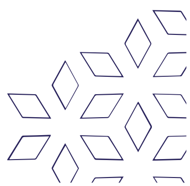
توجد عدة أنواع للاختراقات الأمنية مُقسّمةً حسب كيفية الوصول إلى النظام:

- هجمات استغلال الثغرات تستهدف الثغرات الموجودة في النظام، مثل أنظمة التشغيل غير المُحدَّثة، الأنظمة القديمة التي لم يتم تحديثها، على سبيل المثال، في الشركات التي يتم فيها استخدام إصدارات قديمة من نظام Microsoft Windows والتي لم تعد مدعومة، تكون عرضة بشكل خاص لهجمات استغلال الثغرات.
- يمكن اختراق كلمات المرور الضعيفة أو تخمينها، حتى الآن، لايزال بعض الأشخاص يستخدمون كلمة المرور "password"، كما لاتُعد "pa$$word" أكثر أماناً.
- يمكن استخدام هجمات البرامج الضارة، مثل رسائل التصيّد الاحتيالي عبر البريد الإلكتروني لإيجاد ثغرة للدخول، حيث لا يتطلب الأمر سوى نقر موظف واحد على رابط في رسالة تصيّد احتيالي عبر البريد الإلكتروني، للسماح للبرامج الضارة بالبدء في الانتشار عبر الشبكة.
- تستخدم التنزيلات العرضية الفيروسات أو البرامج الضارة التي تصل من خلال موقع ويب مخترق أو مخادع.
- كما يمكن أيضاً استخدام الهندسة الاجتماعية لاكتساب صلاحية الوصول، كأن يقوم أحد المتسللين مثلاً بالاتصال بموظف ويدعي أنه من مكتب المساعدة في قسم تكنولوجيا المعلومات بالشركة ويطلب كلمة المرور من أجل "إصلاح" الكمبيوتر.

المهاجمين

عبارات بسيطة الهجمات الالكترونية عبارة عن هجوم يتم شنه من أحد أجهزة الكمبيوتر او مجموعة من الاجهزة على جهاز كمبيوتر اخر او عدة أجهزة كمبيوتر او شبكات، **يمكن تقسيم الهجمات الالكترونية (الهجمات السيبرانية) الى نوعين رئيسيين على النحو التالي:**

- هجمات يكمن الهدف من ورائها الى تعطيل جهاز الكمبيوتر المستهدف.
- هجمات يكون الغرض منها الوصول الى بيانات جهاز الكمبيوتر المستهدف وربما الحصول على امتيازات المسئول عنه.



❖ أنواع الهجمات التي تتعرض لها الشبكة

هناك سبعة انواع من الهجمات الالكترونية (الهجمات السيبرانية):

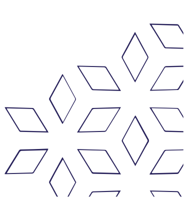
- البرامج الضارة(Malware)
- التصيد(Phishing)
- حجب الخدمات(Denial Of Service)
- الرجل في المنتصف(Man in the middle)
- التعدين الخبيث(Cryptojacking)
- حقن هجومSQL
- هجمات دون انتظار(Zero-Day)

<u>البرامج الضارة Malware</u>

هي اختصار لكلمة برنامج ضار ويمكن ان يشير البرنامج الضار الى اي نوع من البرامج، بصرف النظر عن طريقة تكوينه او تشغيله، وهو "مصمم لإلحاق الضرر بجهاز الكمبيوتر او السيرفر او شبكة جهاز الكمبيوتر مثلما تعرفه : Microsoft إن الفيروسات المتنقلة والفيروسات وحصان طروادة تندرج كلها تحت البرامج الضارة، ولايميزها عن بعضها البعض سوى الوسائل التي يتم استخدامها لإنشائها ونشرها، قد تتسبب هذه الهجمات في تعطيل جهاز الكمبيوتر او الشبكة، او تمكن المهاجم من الوصول حتى يتمكن من التحكم في النظام عن بعد.

<u>التصيد(Phishing)</u>

التصيد تقنية يستخدمها مجرمو الفضاء الإلكتروني في إرسال رسائل بريد إلكتروني لخداع المستهدف من أجل القيام ببعض الأعمال الضارة، ربما يتم خداع المستلم في تنزيل برنامج ضار متخفي في صيغة مستند هام، على سبيل المثال ، او مطالبته بالنقر فوق احد الروابط التي تقوم بتوجيهه الى موقع ويب زائف حيث يتم سؤاله عن معلومات حساسة مثل اسماء المستخدمين وكلمات المرور الخاصة بالبنك، الكثير من رسائل البريد الإلكتروني المتصيدة تكون بدائية الى حد ما ويتم إرسالها الى الالاف من الضحايا المحتملين ، ولكن بعض رسائل البريد الإلكتروني يتم صياغتها وإرسالها بشكل خاص الى افراد مستهدفين ذوي قيمة لمحاولة الوصول على معلومات مفيدة منهم.



حجب الخدمات(Denial Of Service)

هجوم حجب الخدمات هو اسلوب استخدام القوة الغاشمة لمحاولة إيقاف تشغيل بعض الخدمات عبر الإنترنت، على سبيل المثال، قد يقوم المهاجمون بإرسال الكثير من البيانات الى احد مواقع الويب او الكثير من الطلبات الى احدى قواعد البيانات والتي تتسبب في ملئ تلك الأنظمة وتعطيلها عن العمل، وهو ماقد يجعلها غير متاحة لأي شخص، يستخدم هجوم حجب الخدمات الموزعة (DDoS) مجموعة من أجهزة الكمبيوتر، وعادة ماتكون مخترقة عن طريق البرامج الضارة وتحت سيطرة مجرمي الفضاء الإلكتروني ، لإرسال البيانات الى المستهدفين.

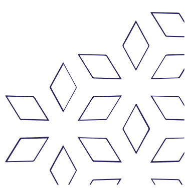
هجمات الرجل في المنتصف(Man In The Middle)

هجوم الرجل في المنتصف (MITM) طريقة ينجح بها المهاجمون في إقحام أنفسهم سرا بين المستخدم وخدمة الويب التي يحاولون الوصول اليها، على سبيل المثال، ربما يقوم المهاجم بإعداد شبكة Wi-Fi مزودة بشاشة تسجيل مصممة بشكل يحاكي احدى شبكات الفنادق وبعد ان يقوم المستخدم بتسجيل الدخول، يمكن ان يجمع المهاجم اي معلومات يرسلها المستخدم، ويشمل ذلك كلمات المرور الخاصة بالبنك الذي يتعامل معه.

التعدين الخبيث(CryptoJacking)

التعدين الخبيث عبارة عن هجوم مخصص وفيه يتم اختراق أحد اجهزة الكمبيوتر الخاصة بأحد الاشخاص واستخدامها لتعدين العملات الرقمية المشفرة (إجراء يطلق عليه التعدين في قاموس مصطلحات عملات التشفير).

سيحاول المهاجمون إما تثبيت أحد البرامج الضارة على جهاز الكمبيوتر الخاص بالضحية لتنفيذ العمليات الحسابية المطلوبة او احياناً تشغيل التعليمة البرمجية في JavaScript والتي يتم تنفيذها في المستعرض الخاص بالضحية.

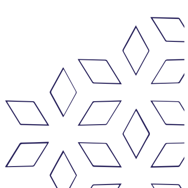


حقنSQL

حقن SQL عبارة عن وسيلة تُمكن المهاجم من استغلال الثغرات في السيطرة على قاعدة بيانات الضحية، توجد العديد من قواعد البيانات المُصممة لتنفيذ أي أوامر مكتوبة في لغة الاستعلامات المركبة (SQL) ، وتقوم العديد من مواقع الويب التي تجمع المعلومات من المستخدمين، بإرسال هذه البيانات إلى قواعد بيانات SQL أثناء الهجوم باستخدام حقن SQL ، سيقوم المخترق، على سبيل المثال، بكتابة بعض أوامر SQL في أحد نماذج الويب التي تطلب معلومات الاسم والعنوان؛ وإذا لم يتم برمجة موقع الويب وقاعدة البيانات بشكلٍ صحيح، فربما تحاول قاعدة البيانات تنفيذ تلك الأوامر.

هجمات دون انتظار (Zero-Day)

الهجمات دون انتظار هي عبارة عن ثغرات في البرامج لم يتم حلها الى الان وسميت كذلك لانه بمجرد إصدار حزمة، يتناقص كل يوم عدد الأجهزة المفتوحة المعرضة للهجوم اثناء تسجيل المستخدم تحديثات الأمان، كثيرا ما يتم شراء وبيع تقنيات استغلال الثغرات هذه على الانترنت المظلم (Dark Web)واحياناً يتم اكتشافها من خلال الوكالات الحكومية التي قد تستخدمها لأغراض الاختراق بدلاً من إصدار معلومات عامة لأجل المنفعة المشتركة.



❖ أمن الشبكات اللاسلكية (عملي)

يعتمد تعريف الأمن إلى حد كبير على السياق، لأن كلمة الأمن تشير إلى طيف واسع من المجالت ضمن وخارج حقل تقنية المعلومات، قد نتكلم مثلاً عن الأمن عند توصيف الجراءات الوقائية على الطرق العامة أو عند استعراض نظام حاسوبي جديد يتمتع بمناعة عالية ضد فيروسات البرمجيات، لقد تم تطوير أنظمة عدة لمعالجة الجوانب المختلفة لمفهوم الأمن.

بناء على ذلك فقد قمنا بصياغة مصطلح "أمن الشبكات اللاسلكية" ضمن تصنيف محدد للأمن بغية تسهيل مهمتنا في دراسة الأمن في مجال الشبكات اللسلكية، تقوم هذه الوحدة بتعريف أمن الشبكات اللاسلكية ضمن سياق أمن المعلومات، أي أننا عندما نتحدث عن أمن الشبكات اللسلكية فإننا نعني أمن المعلومات في الشبكات اللاسلكية.

❖ أمن وسائل نقل المعلومات (عملي)

في التسعينات من القرن الماضي تم دمج مفهومي الأمن (أمن الإتصالات وأمن الحواسيب) لتشكيل ما أصبح يعرف باسم أمن أنظمة المعلومات(Information Systems Security – INFOSEC)

يتضمن مفهوم أمن أنظمة المعلومات الخصائص الأربعة المعرفة مسبقاً ضمن مفاهيم أمن الإتصالات وأمن الحواسيب وهي كالتالي:

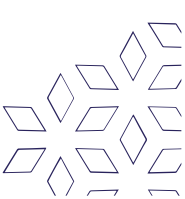
١–السرية.

٢–التحقق من الهوية.

٣–الكمال.

٤–التوفر.

يتضمن مفهوم أمن أنظمة المعلومات أيضاً خاصية جديدة تعرف بمكافحة الإنكار وهي: التأكيد بأن مرسل البيانات قد حصل على إثبات بوصول البيانات إلى المرسل إليه وبأن المستقبل قد حصل على إثبات لشخصية المرسل مما يمنع إحتمال إنكار أي من الطرفين بأنه قد عالج هذه البيانات.



أمن المعلومات في الشبكات اللاسلكية

تعرّف توصيات أمن أنظمة المعلومات والإتصالات لوكالة الأمن القومي في الولايات المتحدة أمن أنظمة المعلومات كما يلي: "حماية أنظمة المعلومات ضد أي وصول غير مرخص إلى أو تعديل المعلومات أثناء حفظها، معالجتها أو نقلها، وضد إيقاف عمل الخدمة لصالح المستخدمين المخولين أو تقديم الخدمة لأشخاص غير مخولين، بما في ذلك جميع الإجراءات الضرورية لكشف، توثيق ومواجهة هذه التهديدات".

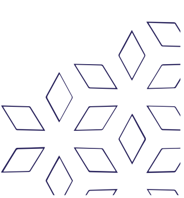
الخصائص الأمنية الخمس في الشبكات اللاسلكية

١-السرية Confidentiality

سنعرّف سرية الشبكات اللاسلكية بضمان أن المعلومات المرسلة بين نقاط الولوج وحواسب المستخدمين لن تصل إلى أشخاص غير مخولين، يجب أن تضمن سرية الشبكات اللاسلكية الأتي: الإتصالات الجارية بين مجموعة من نقاط الولوج ضمن نظام توزيع لاسلكية Wireless Distribution System محمية – الإتصالات الجارية بين نقطة ولوج AP وحاسب متصل بها STA ستبقى محمية.

- **WEP**

-شكلت "السرية المكافئة للشبكة السلكية "WEP جزءاً من المعيار الأساسي IEEE 802.11 للشبكات اللاسلكية في العام ١٩٩٩– إن الهدف الرئيس من السرية المكافئة للشبكة السلكية WEP هو تأمين الشبكات اللاسلكية بمستوى من السرية مماثل للسرية المتوفرة في الشبكات السلكية – لم يستغرق الأمر سوى عدة أشهر من إطلاق البروتوكول حتى تم خرقه وهجرانه – لقد أثبت هذا البروتوكول ضعفه بغض النظر عن طول مفتاح التشفير المستخدم– لقد ساهم عدم توفر نظام لإدارة مفاتيح التشفير ضمن هذا البروتوكول في إفشاله أيضاً– سرعان ما طورت بدائل جديدة لهذا البروتوكول مثل +WEP من شركة Lucent وبروتوكول WEP2 من شركة Cisco - يعتبر بروتوكول السرية المكافئة للشبكة السلكية WEP وتعديلاته +WEP و WEP2 حالياً خارج الخدمة– يعتمد بروتوكول السرية المكافئة للشبكة السلكية على شيفرة سيل RC4 - هناك العديد من البرمجيات المتاحة لاختراق بروتوكول السرية المكافئة للشبكة السلكية منها Airsnort ، wepcrack، kismac، aircrack - إذا ما كنت مهتماً بتاريخ بروتوكول السرية المكافئة للشبكة السلكية ننصحك بمراجعة (موارد إضافية للمعلومات) المرفقة مع هذه الوحدة.



٢-التحقق من الهويةAuthentication

يتم تعريف التحقق من الهوية في سياق الشبكات اللاسلكية بالإجراءات الهادفة لضمان صلاحية الإتصال بين نقاط الولوج والمحطات اللاسلكية، لاستيعاب مفهوم التحقق من الهوية في الشبكات اللاسلكية لا بد من فهم ما يحدث عند بدء جلسة الإتصال بين نقطة الولوج والمحطة اللاسلكية STA.

- **آليات الربط**
- **التحقق المفتوح من الهوية:**

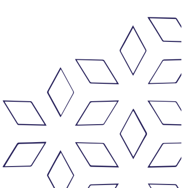
-لا يوجد أي آلية للأمن مما يمكن أي شخص كان من الإتصال مع نقطة الولوج.

- **التحقق من الهوية باستخدام المفتاح المشترك:**

-يتم تشارك سر (كلمة سر) بين محطة المستخدم ونقطة الولوج– تتيح آلية طلب الإستجابة للتحدي لنقطة الولوج بالتحقق من أن المستخدم يعرف السر المشترك وستسمح له بالتالي الوصول إلى الشبكة اللاسلكية.

بروتوكول السرية المكافئة للشبكة السلكية والتحقق من الهوية في الطبقة الثانية:

-تعتبر آلية التحقق من الهوية باستخدام مفتاح التشفير المشترك والمستخدمة في بروتوكول السرية المكافئة للشبكة اللاسلكية WEP بائدةً – يمكن بسهولة اختراق آلية التشفير المستخدمة في بروتوكول WEP باستخدام هجمات نصوص تشفير بسيطة – مفتاح التشفير ومفتاح التحقق من الهوية يستخدمان نفس السر المشترك – فإن اكتشاف أي من هذين المفتاحين سيؤدي إلى اكتشاف الآخر.



بعض النصائح عن بروتوكول السرية المكافئة للشبكة السلكية والتحقق من الهوية في الطبقة الثانية:

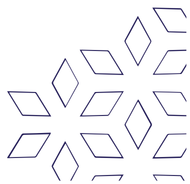
-استخدم النمط المؤسساتي لبروتوكول - WPA2 يتم تنفيذ التحقق من الهوية في الشبكات اللاسلكية عادة (كما في حال مزودي خدمات الإنترنت اللاسلكية) ضمن الطبقات الأعلى لنموذج OSI (المرجعي) طبقة بروتوكول الإنترنت IP عبر بوابات مقيدة (أي تسجيل الدخول إلى موقع للإنترنت) – لا بد من الإنتباه إلى أنه عند نقل وظائف التحقق من الهوية إلى "بوابات مقيدة" فإننا سنفقد القدرة على إيقاف انتقال البيانات التي تعبر نقط الولوج الخاصة بنا.

- **استخدام فلترة العناوين الفيزيائية كإجراء لتعزيز أمن الشبكة اللاسلكية:**

-يستخدم الكثير من مزودي خدمات الإنترنت اللاسلكية فلترة العنوان الفيزيائي لبطاقة الشبكة اللاسلكية كآلية لتحديد أو توفير الوصول إلى الشبكة اللاسلكية على اعتبار أن العناوين الفيزيائية MAC مسجلة ضمن المكونات الإلكترونية لبطاقة الشبكة وبالتالي يستحيل تغييرها من قبل المستخدمين العاديين، المشكلة يمكن ببساطة تغيير العناوين الفيزيائية في معظم بطاقات الشبكة اللاسلكية لايمكن اعتبار أية آلية للتحقق من الهوية تعتمد فقط على العناوين الفيزيائية MAC إجراء آمناً.

- **البوابات المقيّدة للشبكات اللاسلكية:**

-يسمح لمستخدمي الشبكة بالربط مع أية نقطة ولوج والحصول على عنوان إنترنت IP عبر بروتوكول الإعداد التلقائي للمضيف - DHCP بعد حصول المستخدم على عنوان إنترنت IP ستقوم الشبكة بالتقاط جميع طلبات الوصول إلى الإنترنت عبر بروتوكول HTTP لإجبار المستخدم على "تسجيل الدخول" إلى صفحة إنترنت – تضطلع البوابات المقيّدة بمهمة التأكد من صحة كلمة السر التي أدخلها المستخدم وتعديل حالة الجدار الناري (والذي غالباً ما يتوضع ضمن نفس الجهاز) – تعتمد قواعد الجدار الناري على قيم العنوان الفيزيائي MAC وعنوان الإنترنت IP الذي حصل عليه المستخدم عبر بروتوكول DHCP .



٣-الكمال Integrity

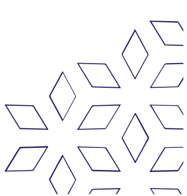
-قدرة بروتوكول الإتصال اللاسلكي على كشف أي تحريف في البيانات المنقولة من قبل أشخاص غير مخولين – كان من المفترض ببروتوكول السرية المكافئة للشبكة السلكية WEP أن يضمن كمال البيانات المنقولة– إن آلية كمال البيانات المستخدمة في بروتوكول WEP التحقق الدوري من الأخطاء (Cyclic Redundancy Check – CRC) لم تكن آمنة أمر متوقع – يمكن تعديل البيانات المنقولة وتحديث قيمة CRC الخاصة بهذه البيانات حتى دون معرفة مفتاح تشفير WEP .

النتيجة

يمكن تحريف البيانات المنقولة دون أن يتم يكشف هذا التحريف.

WPA و WPA2 تضمنت شيفرةً أكثر أمناً للتحقق من الرسالة إضافةً إلى عدادٍ للإطارات والذي يمنع ما يسمى بـ "هجمات الإعادة"Replay Attacks .

WPA مقارنةً مع WPA2 يعتبر كمال البيانات عبر بروتوكول WEP منقرضاً يجب استخدام بروتوكول الوصول المحمي للشبكة اللاسلكية WPA أو WPA2 لتحقيق كمال البيانات في الشبكات اللاسلكية عبر التشفير على مستوى الوصلة.



٤-التوفر Availability

هي قدرة التقنية على ضمان الوصول الموثوق إلى خدمات البيانات والمعلومات للمستخدمين المخولين.

- **التشويش على القنوات الراديوية للشبكات اللاسلكية:**

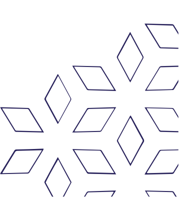
–عنصر أ تعمل الشبكات اللاسلكية ضمن نطاقٍ محدد للقنوات الراديوية يمكن استخدامه من قبل أي شخص لإرسال إشارات لاسلكية.

–عنصر ب من شبه المستحيل منع الأشخاص غير المخولين من التشويش على شبكتك.

–عنصر ج نصيحة يجب مراقبة الوصلات اللاسلكية بعناية وذلك بغرض تحديد المصادر المحتملة للتشويش.

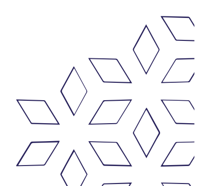
٥-مكافحة الإنكار – المسؤولية

لا تحتوي بروتوكولات الشبكات اللاسلكية على آليةٍ للتأكيد على أن مرسل البيانات قد حصل على إثبات لتسلم المستقبل لرسالته أو على أن المستقبل قد حصل على إثبات لهوية المرسل – يجب إعداد المسؤولية ضمن بروتوكولات الطبقات العليا.



❖ الشبكات المحلية الإفتراضية وأمنها

الشبكة المحلية الافتراضية، هي أي نطاق بث مجزأ ومعزول داخل شبكة الحاسوب ضمن طبقة ربط البيانات حتى نستطيع تقسيم الشبكة إلى شبكات محلية وهمية، يحتاج الشخص إلى فهم الشبكة وطريقة ربط معداتها، هنالك معدات بسيطة يمكن استخدامها للتجزئة من خلال المنافذ الموجودة على الجهاز نفسه (إذا وجدت), وفي هذه الحالة كل شبكة محلية وهمية يتم شبكها بكيبل مخصص لها، اما بالنسبة للاجهزة الأكثر تطورا فانها تتمتع بالقدرة على تحديد frames من خلال تقنية vlan tagging, بحيث انه يمكن لبروتوكول الشبكات الافتراضية الوهمية الجذعي ان يستخدم لنقل البيانات لاكثر من شبكة محلية وهمية، بما ان الشبكات المحلية الوهمية تتشارك عرض النطاق الترددي فان بروتوكول الشبكات الافتراضية الوهمية الجذعي يستخدم جمع الوصلات تحديد اولية مستوى الخدمة، أو كليهما لتحديد اتجاه نقل البيانات بكفاءة، تسمح الشبكات المحلية الوهمية لمسؤولين الشبكات بجمع المتصلين على الشبكة مع بعض حتى وان كانوا هؤلاء المتصلين بالشبكة ليسوا ضمن نطاق الشبكة الواحدة، وهذا ييسط بطريقة كبيرة تصميم الشبكة ونشرها، لان الشبكة المحلية الوهمية يمكن ان يتم تصميمها من خلال البرمجة، بدون وجود الشبكات المحلية الوهمية عملية جمع وربط المتصلين بالشبكات بالاعتماد على نقاط اتصالهم ستحتاج إلى تحديد نقطة اتصالهم واعادة توجيه هذه النقاط واسلاك اتصالهم، وهذه العملية حقا صعبة وغير عملية.



❖ الاتصال الآمن بالإنترنت (عملي)

ما المقصود بالأمن على الإنترنت؟ - التعريف والمعنى

أمان الإنترنت هو مصطلح يصف أمن الأنشطة والمعاملات التي تتم عبر الإنترنت، إنه مكون خاص من الأفكار الأكبر للأمن الإلكتروني وأمن الكمبيوتر، بما في ذلك موضوعات تشمل أمان المتصفح والسلوك عبر الإنترنت وأمن الشبكة، إننا نقضي جزءاً كبيراً من حياتنا على الإنترنت،

وتشمل التهديدات التي قد تواجهنا إزاء أمن الإنترنت ما يلي:

- التسلل، والذي يعرف أيضاً باسم القرصنة، حيث يتمكن المستخدمون غير المصرح لهم من الوصول إلى أنظمة الكمبيوتر أو حسابات البريد الإلكتروني أو مواقع الويب.
- الفيروسات أو البرامج الضارة (المعروفة باسم البرمجيات الضارة) التي يمكنها إتلاف البيانات أو جعل الأنظمة عرضة للتهديدات الأخرى.
- سرقة الهوية، حيث يمكن للمجرمين سرقة المعلومات الشخصية والمالية.

يستطيع الأفراد والمؤسسات حماية أنفسهم من هذه الأنواع من التهديدات من خلال اتباع سبل حفظ الأمن على الإنترنت.

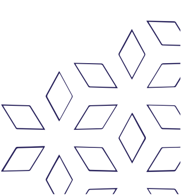
ما هي أكثر تهديدات أمن الإنترنت شيوعاً؟

لضمان الخصوصية والأمان على الإنترنت، من المهم أن تكون على دراية بالأنواع المختلفة من الهجمات التي تتم عبر الإنترنت، **تشمل تهديدات أمن الإنترنت الشائعة ما يلي:**

<u>التصيُّد الاحتيالي</u>

التصيُّد الاحتيالي هو هجوم إلكتروني يمارس عبر رسائل بريد إلكتروني متنكرة، يحاول المتسللون خداع مستلمي البريد الإلكتروني للاعتقاد بأن الرسالة حقيقية وأن شأنها يعنيهم، كأن تتنكر في صيغة طلب من مصرفهم أو ملاحظة من زميل في العمل مثلاً ، بحيث ينقرون على رابط أو يفتحون مرفقاً، والهدف من ذلك هو خداع الأشخاص ليقوموا بالكشف عن معلوماتهم الشخصية أو تنزيل برامج ضارة.

يعد التصيُّد الاحتيالي أحد أقدم تهديدات أمن الإنترنت، ويعود تاريخه إلى التسعينيات من القرن الماضي، على أنه قد ظل شائعًا حتى يومنا هذا؛ لأنه أحد أرخص الطرق وأسهلها على المجرمين لسرقة المعلومات. وفي السنوات الأخيرة، أصبحت تقنيات ورسائل التصيُّد الاحتيالي أكثر تعقيداً.



التسلل والوصول عن بُعد

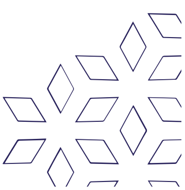
يسعى المتسللون دائماً إلى استغلال نقاط ضعف الشبكة أو النظام الخاصة حتى يتمكنوا من سرقة المعلومات والبيانات السرية، وتمنحهم تقنية الوصول عن بُعد هدفاً آخر يمكنهم استغلاله، إذ يسمح برنامج الوصول عن بُعد للمستخدمين بالوصول إلى جهاز الكمبيوتر والتحكم فيه عن بُعد، ومنذ انتشار الجائحة، ومع زيادة عدد الأشخاص الذين يعملون عن بُعد، ازداد استخدامه.

يسمى البروتوكول الذي يسمح للمستخدمين بالتحكم في جهاز كمبيوتر متصل بالإنترنت عن بُعد بروتوكول سطح المكتب البعيد أو(RDP) ، نظراً لأن الشركات من جميع الأحجام تستخدم RDP على نطاق واسع، فإن فرص وجود شبكة مؤمنة تأميناً غير موثوق مرتفعة نسبياً، يستخدم المتسللون تقنيات مختلفة لاستغلال ثغرات RDP حتى يتمكنوا من الوصول الكامل إلى الشبكة وأجهزتها، وقد يقومون بسرقة البيانات بأنفسهم أو يبيعون بيانات الاعتماد على شبكة الويب المظلمة.

البرمجيات الضارة والإعلانات الضارة

"البرمجيات الضارة" عبارة عن مصطلح مفرداته "برامج الكمبيوتر" و"الضرر الإلكتروني". وهو مصطلح واسع يتعلق بالفيروسات والفيروسات المتنقلة وأحصنة طروادة والبرامج الضارة الأخرى التي يستخدمها المتسللون للتسبب في الفوضى والتخريب وسرقة المعلومات الحساسة، يمكن وصف أي برنامج يهدف إلى إتلاف جهاز كمبيوتر أو خادم أو شبكة على أنه برنامج ضار.

"الإعلانات الضارة" عبارة عن مصطلح مفرداته "الإعلان" و"الضرر" وهو يشير إلى الإعلان عبر الإنترنت الذي يوزع البرامج الضارة، يُعد الإعلان عبر الإنترنت نظاماً معقداً يتضمن مواقع الناشرين وتبادل الإعلانات وخوادمها وشبكات إعادة الاستهداف وشبكات توصيل المحتوى، يستغل المخترقون عبر الإعلانات هذا التعقيد لوضع تعليمات برمجية ضارة في أماكن لا يكتشفها الناشرون وشبكات الإعلانات دائماً، ويمكن لمستخدمي الإنترنت الذين يتفاعلون مع إعلان ضار تنزيل برامج ضارة على أجهزتهم أو أن تتم إعادة توجيههم إلى مواقع ويب ضارة.



برامج طلب الفدية

برنامج طلب الفدية هو نوع من البرامج الضارة التي تمنعك من استخدام جهاز الكمبيوتر الخاص بك أو الوصول إلى ملفات معينة عليه ما لم تدفع فدية، غالباً ما يتم توزيع هذه البرامج كأحصنة طروادة، أي برامج ضارة متخفية كبرنامج مشروع أو أصيل، لكن بمجرد التثبيت، يقفل البرنامج شاشة نظام التشغيل أو ملفات معينة إلى أن تدفع.

يحدد مشغلو برامج طلب الفدية عادةً الدفع بالعملات المشفرة، مثل Bitcoin ، على سبيل حماية إخفاء هوياتهم كما يظنون،وتختلف مبالغ الفدية اعتمادًا على نوع برامج طلب الفدية وسعر أو سعر صرف العملات الرقمية، ليس من المضمون دائمًا أن يقوم المجرمون بالإفراج عن الملفات المشفرة حال دفعك للفدية.

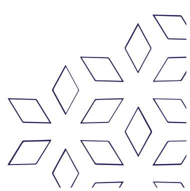
تتزايد هجمات برامج الفدية الضارة، وتستمر أنواع برامج طلب الفدية الجديدة في الظهور، وتتضمن أنواع برامج الفدية الأكثر شيوعاً Maze :و Conti و GoldenEye و Bad Rabbit و Jigsaw و Locky و WannaCry.

شبكات بوت نت

مصطلح بوت نت هو اختصار "الشبكة الروبوتية" الشبكة الروبوتية عبارة عن شبكة من أجهزة الكمبيوتر التي تم إصابتها عن قصد ببرامج ضارة حتى تتمكن من تنفيذ المهام الآلية على الإنترنت دون إذن أو معرفة مالكي أجهزة الكمبيوتر.

وبمجرد أن يتحكم مالك الروبوتات في جهاز الكمبيوتر الخاص بك، يمكنه استخدامه لتنفيذ أنشطة ضارة. ومن بينها:

- توليد حركة مرور وهمية على الإنترنت على مواقع الطرف الثالث لتحقيق مكاسب مالية.
- استخدام قوة جهازك للمساعدة في هجمات رفض الخدمة الموزعة (DDoS) لإغلاق مواقع الويب.
- إرسال بريد إلكتروني عشوائي إلى ملايين مستخدمي الإنترنت.
- الاحتيال وسرقة الهوية.
- مهاجمة أجهزة الكمبيوتر والخوادم.



تصبح أجهزة الكمبيوتر جزءاً من الروبوتات بنفس الطرق التي تُصاب بها بأي نوع آخر من البرامج الضارة، على سبيل المثال، يتم هذا من خلال فتح مرفقات البريد الإلكتروني التي تقوم بتنزيل برمجيات ضارة أو زيارة مواقع الويب المصابة بالبرمجيات الضارة، كما يمكنها أيضاً الانتشار من كمبيوتر إلى آخر عبر الشبكة، يختلف عدد الروبوتات في الشبكة الروبوتية ويعتمد على قدرة مالك الروبوتات على إصابة الأجهزة غير المحمية.

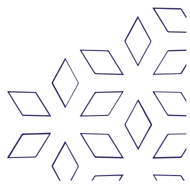
تهديدات شبكةWi-Fi في الأماكن العامة وفي المنزل

تنطوي شبكات Wi-Fi العامة على مخاطر لأن الأمن على هذه الشبكات في المقاهي ومراكز التسوق والمطارات والفنادق والمطاعم وما إلى ذلك غالباً ما يكون ضعيفاً أو حتى غير موجود بالمرة، ويعني الافتقار إلى الأمان أن المجرمين الإلكترونيين ولصوص الهوية يمكنهم مراقبة ما تفعله عبر الإنترنت وسرقة كلمات المرور والمعلومات الشخصية الخاصة بك.

تشمل مخاطر Wi-Fi العامة الأخرى:

- اكتشاف الحزم يقوم المهاجمون بمراقبة البيانات غير المشفرة واعتراضها أثناء انتقالها عبر شبكة غير محمية.
- هجمات الوسطاء يقوم المهاجمون باختراق نقطة اتصال شبكة Wi-Fi لإقحام أنفسهم في الاتصالات بين الضحية المستهدفة ونقطة الاتصال لاعتراض البيانات أثناء النقل وتعديلها.
- شبكات Wi-Fi المخادعة يقوم المهاجمون بإعداد نقطة جذب على شكل شبكة Wi-Fi مجانية لجمع البيانات القيمة، تصبح نقطة اتصال المهاجم هي قناة الممر لجميع البيانات التي يتم تبادلها عبر الشبكة.

ربما لا يوجد داعٍ للقلق كثيراً بشأن تجسس شخص ما على شبكة Wi-Fi في المنزل لأنك تمتلك أجهزة الشبكة ذاتها، ومع ذلك، تظل هناك تهديدات. في الولايات المتحدة الأمريكية، يُسمح لمزودي خدمة الإنترنت (ISP) ببيع بيانات بشأن مستخدمي خدماتهم، وفي حين أن البيانات مجهَّلة الهوية، إلا أن الفكرة تظل مقلقة لأولئك الذين يقدّرون قيمة الخصوصية والأمان على الإنترنت، يصَّعب استخدام الشبكة الافتراضية الخاصة (VPN) في المنزل على الغرباء ربط نشاطك عبر الإنترنت بك.



❖ التدابير الأمنية العامة لأمن شبكات الحاسب

كيفية حماية بياناتك على الإنترنت

إذا كنت تتساءل عن كيفية ضمان الحماية بشكل عام على الإنترنت ولا سيَّما حماية بياناتك، فستجد فيما يلي بعضاً من نصائح أمان الإنترنت المعقولة التي يمكنك اتباعها:

<u>قم بتمكين المصادقة متعددة العناصر أينما أمكنك ذلك</u>

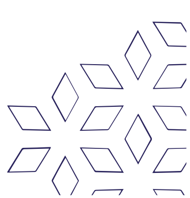
المصادقة متعددة العناصر (MFA) هي طريقة للمصادقة تطلب من المستخدمين توفير طريقتين أو أكثر من طرق التحقق للوصول إلى حساب عبر الإنترنت، على سبيل المثال، بدلاً من مجرد طلب اسم مستخدم أو كلمة مرور، تذهب المصادقة متعددة العناصر إلى أبعد من ذلك من خلال طلب معلومات إضافية، **مثل**:

- كلمة مرور إضافية تُستخدم مرة واحدة، ترسلها خوادم مصادقة موقع الويب إلى هاتف المستخدم أو عنوان بريده الإلكتروني.
- إجابات عن أسئلة الأمان الشخصية.
- بصمة الإصبع أو غيرها من المعلومات الحيوية، مثل الصوت أو التعرف على الوجه.

تقلل المصادقة المتعددة العناصر من احتمالية حدوث هجوم إلكتروني ناجح، لجعل حساباتك على الإنترنت أكثر أماناً، من الأفضل تنفيذ مصادقة متعددة العناصر حيثما أمكن ذلك، يمكنك أيضاً التفكير في استخدام تطبيق مصادقة تابع لجهة خارجية، مثل Google Authenticator و Authy للمساعدة في التمتع بالأمن على الإنترنت.

<u>استخدام جدار حماية</u>

يعمل جدار الحماية كحاجز بين جهاز الكمبيوتر الخاص بك وشبكة أخرى، مثل الإنترنت، تحجب جدران الحماية حركة المرور غير المرغوب فيها ويمكن أن تساعد أيضاً في منع البرمجيات الضارة من إصابة جهاز الكمبيوتر، غالباً ما يكون نظام التشغيل ونظام الأمان لديك مزوداً بجدار حماية مثبت مسبقاً، وإنها لفكرة جيدة أن تتأكد من تشغيل هذه الميزات، مع تكوين إعداداتك لإجراء التحديثات تلقائياً، لزيادة أمن الإنترنت إلى أقصى حد.



الحذر عند اختيار المستعرض

المستعرضات هي بواباتنا الأساسية إلى الويب، وبالتالي تلعب دوراً رئيسياً في الأمن على الإنترنت، يجب أن يكون مستعرض الويب الجيد آمناً ويساعد على حمايتك من انتهاكات البيانات، قامت مؤسسة Freedom of the Press بتجميع دليل مفصل هنا، يشرح إيجابيات الأمان مستعرضات الويب الرائدة في السوق وسلبياتها.

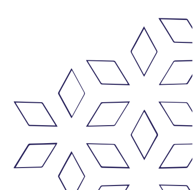
إنشاء كلمات مرور قوية واستخدام مدير كلمات مرور آمن

ستساعدك كلمة المرور القوية في الحفاظ على أمنك على الإنترنت، تتصف كلمة المرور الجيدة بما يلي:

- طويلة – تتكون من ١٢ حرفاً على الأقل، وُفضل أطول من ذلك.
- مزيج من الأحرف أي تشمل أحرفاً كبيرة وصغيرة بالإضافة إلى الرموز والأرقام.
- تتجنب الاحتمالات الواضحة مثل استخدام الأرقام المتسلسلة ("١٢٣٤") أو المعلومات الشخصية التي قد يخمنها شخص يعرفك، مثل تاريخ ميلادك أو اسم حيوانك الأليف.
- تتجنب تراتيب أزرار لوحة المفاتيح السهل تذكرها.

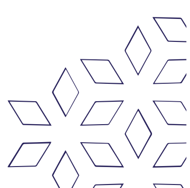
في هذه الأيام، لم يعد من الكافي استبدال الأحرف المتشابهة بالأحرف أو الأرقام على سبيل المثال، "P@ssw0rd" بدلاً من "password" نظراً لأن المخترقين أذكياء في التعامل مع هذه الطرق، كلما كانت كلمة مرورك أكثر تعقيدًا وخصوصية، بات من الصعب اختراقها، سيساعدك استخدام مدير كلمات المرور من خلال إنشاء جميع كلمات المرور الخاصة بك وتخزينها وإدارتها في حساب واحد آمن عبر الإنترنت.

حافظ على خصوصية كلمات مرورك بأن تتجنب مشاركتها مع الآخرين أو كتابتها، حاول تجنب استخدام كلمة المرور نفسها لجميع حساباتك وتذكر أن تغيرها بانتظام.



احتفظ ببرنامج أمان محدث مثبتاً على أجهزتك

يعد برنامج مكافحة فيروسات لحفظ أمنك على الإنترنت أداة بالغة الأهمية لضمان الخصوصية والأمان، سيحميك أفضل برنامج لأمن الإنترنت من أنواع مختلفة من هجماته ويحمي بياناتك عبر الاتصال به، ومن المهم لأن تحرص على تحديث برامج مكافحة الفيروسات باستمرار، كما تقوم معظم البرامج الحديثة بتحديث نفسها تلقائياً للبقاء على اطلاع بأحدث تهديدات الأمن على الإنترنت.



سادساً: الهندسة الاجتماعية

في هذا الفصل سنتعرف على المواضيع التالية:

- مفهوم الهندسة الاجتماعية وأهدافها
- أنواع الهندسة الاجتماعية
- جوانب الهجمات بأسلوب الهندسة الاجتماعية
- أساليب الهجوم بإستخدام الهندسة الاجتماعية
- الأثار المترتبة على الهندسة الاجتماعية
- إجراءات الحد من مخاطر الهندسة الاجتماعية
- طرق رئيسية لحماية الأجهزة والمعلومات من الإختراق

❖ مفهوم الهندسة الاجتماعية وأهدافها

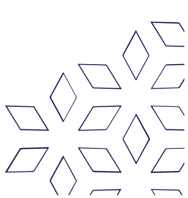
في كتاب Social Engineering أو الهندسة الاجتماعية، يتحدث الكاتب الأمريكي كرستوفر هادناجي عن الهندسة الاجتماعية للهكر وفن اختراق العقل البشري، ويعرفها على أنها مجموعة من الأنماط والسلوكيات البشرية التي نمارسها بقصد أو دون قصد، والتي يستخدمها المختصون عامة في التسويق لإقناع الجمهور بمنتج بعينه والترويج لمؤسسات، كما تستخدم في عالم السياسة من أجل كسب تأييد الجماهير، كما يستخدمها الأطباء في بعض الأحيان لحث مرضاهم على اتباع نظام غذائي معين على سبيل المثال من أجل صحتهم.

أما الجانب السلبي لل الهندسة الاجتماعية هى أن المحتالين وعصابات الاختراق الإلكتروني تستخدمها من أجل استغلال نقاط الضعف في عقلية المستخدم من أجل تحقيق أهدافهم وتوجيه الأشخاص على شبكة الإنترنت لتنفيذ خططهم التخريبية، لذلك نجد أن القرصنة الإلكترونية تعتمد اعتماداً أساسياً على هذا العلم.

وبالتالي فإن المهندسين الاجتماعيين قد يكونوا هم الأشخاص المعنيين بحماية أمن البيانات وحفظ المعلومات إلكترونياً عن يد المخربين، ومن الممكن أيضاً أن يكونوا هم أنفسهم المخربين، وفي هذه الحالة يكون تأثيرهم أكثر خطورة من القرصنة.

كيف تعمل الهندسة الاجتماعية؟

تعتمد معظم هجمات الهندسة الاجتماعية على التواصل الفعلي بين المهاجمين والضحايا، حيث يميل المهاجم لخداع المستخدم من خلال تحفيزه لأداء مهمة معينة تعرضه من خلالها للاختراق، بدلاً من استخدام الأساليب الواضحة لاختراق بياناتك من خلال استغلال نقاط الضعف في البرامج وانظمة التشغيل، لذلك، تعد هجمات الهندسة الاجتماعية مفيدة بشكل خاص للتلاعب بسلوك المستخدم، بمجرد أن يفهم المهاجم ما الذي يحفز تصرفات الضحية، يمكنه خداعه والتلاعب به بشكل فعال.

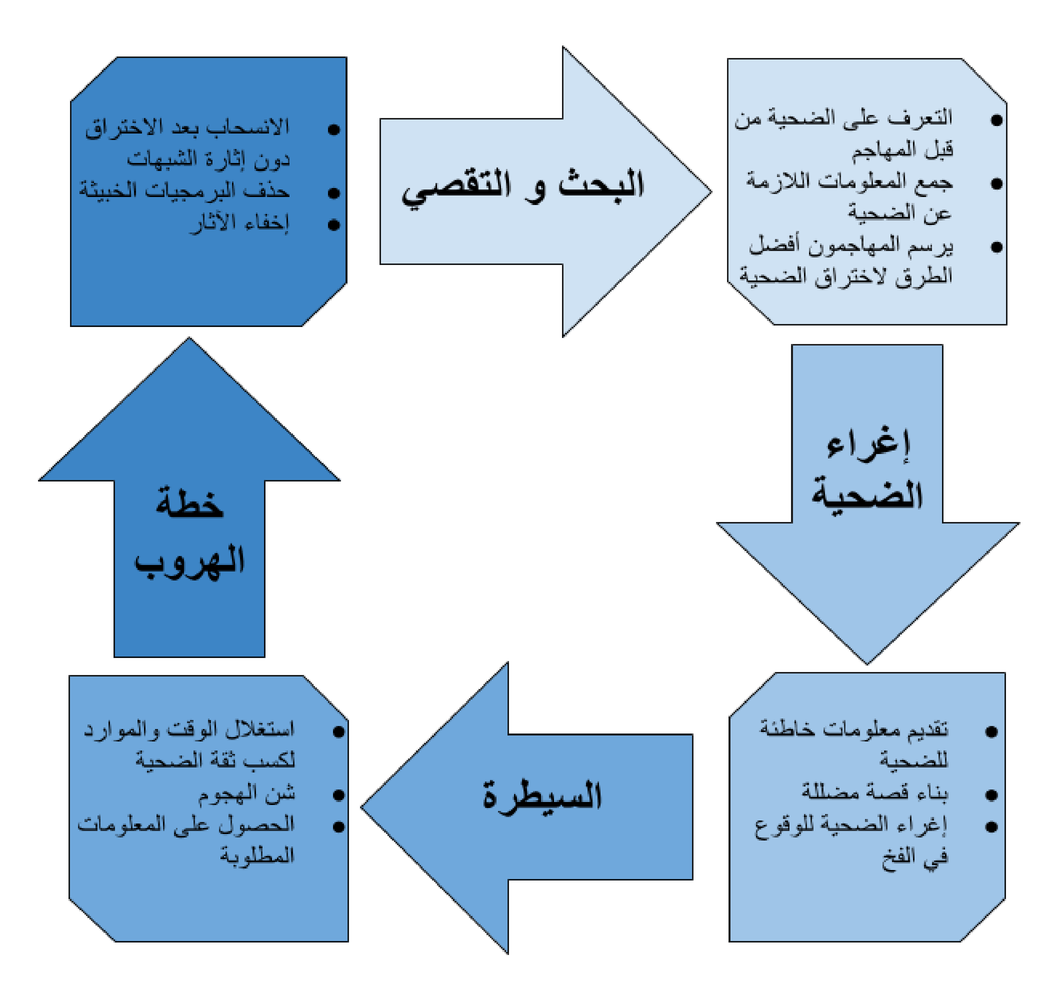


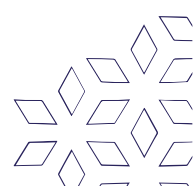
عادة ما تكون خطوات دورة هجوم الهندسة الاجتماعية كما يلي:

- جمع معلومات أساسية عنك أو عن مجموعة أكبر أنت جزء منها.
- تسلل من خلال تواصل يبدأ ببناء الثقة.
- استغلال الضحية بمجرد أن تنشأ الثقة لتعزيز الهجوم.
- قطع العلاقة بالضحية بمجرد أن يتخذ الضحية الإجراء المطلوب.

يمكن أن تتم هذه العملية في رسالة بريد إلكتروني واحدة أو على مدار أشهر في سلسلة من محادثات عبر الوسائل الاجتماعية، كما يمكن أن يكون تفاعلًا وجهاً لوجه، ينتهي في النهاية بالحصول على بيانات حساسة او اجراء معين ينفذه الضحية، مثل مشاركة معلومات مهمة أو تنزيل برامج ضارة.

لا يدرك العديد من الموظفين والمستهلكين أن مجرد معلومات بسيطة يمكن أن تمنح المتسللين إمكانية الوصول إلى شبكات وحسابات متعددة.





❖ أنواع الهندسة الاجتماعية

بالتأكيد يوجد أنواع للهندسة الاجتماعية والتي يستخدمها المقرصنون من أجل اختراق العقول والحصول على المعلومات الكافية للإيقاع بالضحية وسرقة بياناته وفي أحيان كثير أمواله، وهنا سنوضح أشهر أنواع الهندسة الاجتماعية.

اصطياد الضحية

يستغل المقرصن في هذه الحالة فضول الضحية، فيقدم له أحد الوعود الكاذبة من أجل الإيقاع بالضحية في المصيدة وسرقة بياناته الشخصية أو التلاعب بالنظام الأمني من خلال إرسال رابط يحمل فيروس إلكتروني ليبدأ في سحب البيانات من الجهاز الإلكتروني.

وليس بالضرورة أن تحدث محادثة فعلية بين المقرصن وضحيته، ولكنه يكفي أن ينشر إعلان على مواقع إلكترونية مختلفة، تحمل رسالة تجذب انتباه المستخدم للضغط على الرابط أو تحميل تطبيق يكون نافذة هذا المهندس لاختراق الجهاز.

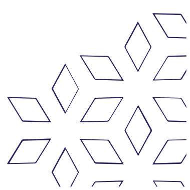
سكير وير Scarware

نوع أخر من أشكال البرمجيات الخبيثة، والتي غالباً ما تتضمن إنذار كاذب بوجود فيروس اختراقي لجهازك، أو تهديد بأن جهازك مراقب، والتي توجه المستخدمين لتحميل برنامج لحماية جهازك، والذي يكون هذا البرنامج هو التهديد بحد ذاته.

الهجوم الإلكتروني Pretexting

نوع آخر يستخدمه المقرصنون من أجل الحصول على البيانات الشخصية للطرف الآخر سواء إلكترونياً أو باستخدام أي وسيلة للتواصل مع الضحية مثل هاتفياً، بإرسال رسالة نصية ينتحل فيه المقرصن شخصية أخرى، ويسعى لاستخراج البيانات من الضحية.

وهنا يحاول المهاجم إقناع المستخدم بضرورة مشاركة تلك البيانات من أجل إجراء مهمة عاجلة شديدة الأهمية.



❖ جوانب الهجمات بأسلوب الهندسة الاجتماعية

تتمحور هجمات الهندسة الاجتماعية حول استخدام المهاجم للإقناع والثقة، عندما تتعرض لهذه التكتيكات، فمن المرجح أن تتخذ إجراءات دون إدراكك أو التفكير في مدى خطورتها.

في معظم هجمات الهندسة الاجتماعية، يقوم المهاجم بالتلاعب بالضحية واقناعه من خلال:

<u>التلاعب بالمشاعر:</u>

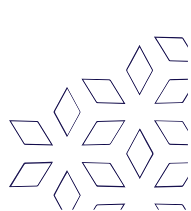
يمنح التلاعب العاطفي للمهاجمين اليد العليا في أي تفاعل، أنت أكثر عرضة لاتخاذ إجراءات غير عقلانية أو محفوفة بالمخاطر عندما تكون في حالة عاطفية محسّنة، يتم استخدام جميع المشاعر التالية (الخوف – الاثارة – حب الاستطلاع – الغضب – الذنب – حزن) بشكل متوازي لإقناعك.

<u>الاستعجال:</u>

الفرص أو الطلبات الحساسة للوقت هي أساليب أخرى يستخدمها المهاجم في هجمات الهندسة الاجتماعية، قد يقوم المخترق بأقناعك بوجود مشكلة خطيرة تحتاج إلى اهتمام فوري واتخاذ اجراء سريع فهنا لايكون عناك وقت للتفكير حيث يستخدم هذا التكتيك في الهندسة الاجتماعية لتشتيت تفكيرك وتحفيزك لتنفيذ شيء معين او قد يتم تحفيزك من خلال جائزة أو مكافأة قد تختفي إذا لم تتصرف بسرعة مثل العروض الاحتيالية، كلا الأسلوبين يتجاوز قدرتك على التفكير بعمق ويتسبب بتشتيت تفكيرك.

<u>الثقة:</u>

المصداقية لا تقدر بثمن وضرورية لهجوم الهندسة الاجتماعية، نظراً لأن المهاجم يكذب عليك في النهاية، فإن الثقة تلعب دوراً مهماً هنا، حيث يقوم المهاجم بإجراء أبحاثًا كافية عنك لصياغة قصة يسهل عليك تصديقها ومن غير المرجح أن تثير الشكوك.



❖ أساليب الهجوم بإستخدام الهندسة الاجتماعية

١-جمع المعلومات

باختلاف نوايا المهندس الاجتماعي وأغراضه، فإن ما يبحث عنه هو المعلومات، فمهما كانت تلك المعلومات بسيطة، فهو يدرك أهمية حفظها، فربما قد يحتاجها مستقبلاً.

لذلك فهو يرسخ كل تركيزه عن كيفية جمع تلك المعلومات وتنظيمها، ثم تحليلها لمعرفة ما يمكن استنتاجه من هذا الكم من البيانات الذي أصبح متوفر على شبكة الإنترنت ومواقع التواصل الاجتماعي.

٢-تقديم حقائق واستنتاجات

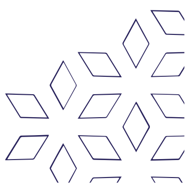
يبدأ المهندس الاجتماعي في ترتيب تلك المعلومات واستخدام أدوات خاصة لتحليلها من أجل الحصول على حقائق واستنتاجات ذو مغزى.

فأحيانًا يبدأ المهندس الاجتماعي في إجراء محادثات مع ضحاياه تبدو صادقة وودودة، ولكنه في الوقت ذاته يبدأ في استخلاص المعلومات منه دون أن يشعر الطرف الآخر بأي مصدر تهديد له، فغالباً ما يكون محترفي الهندسة الاجتماعية أشخاص يتمتعون بسرعة البديهة والإنصات للآخرين.

وتتبع تلك السياسة أغلب أجهزة الاستخبارات العالمية وذلك من أجل كسب ثقة الطرف الأخر وإرضاء غروره، ومن ثم يبدأ في الحديث عن الكثير من المعلومات المهمة سواء عن حياته أو عن الأشخاص الذين يعرفهم.

٣-انتحال الهوية

من أكثر السبل انتشارًا في الفضاء الإلكتروني، كما أنها أخطرها، حيث ينتحل هذا المهندس أو المقرصن شخصية أخرى من أجل استخلاص المعلومات من الطرف الأخر، وذلك بالطبع بعد أن يجمع المهندس كافة المعلومات اللازمة عن تلك الشخصية حتى يتمكن من الرد بعفوية وسريعاً على أي سؤال أو استفسار، وحتى يقنع الضحية بخدعته حتى يحصل على ما يريد.



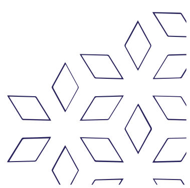
❖ الآثار المترتبة على الهندسة الاجتماعية

تُعتبر الهندسة الاجتماعية الطريقة الأسرع والأقوى لكسب معلومات ذات قيمة كبيرة عن الأشخاص بشكل عام، حيث يقوم المُهاجم باستخدام المعلومات القليلة التي يملكها ليكسب ثقة ضحيته، وبواسطة هذه الثقة ينتهي الأمر بالضحية أن يقدم للمُهاجم معلومات حساسة يستطيع من خلالها اكتشاف خصائص النظام.

وهناك أساليب يمكن أن يتم إيقاع الضحايا بها، مثل الهاتف، حيث أكثر الهجمات الهندسة الاجتماعية تقع عن طريق الهاتف، وحتى يتمكن الفرد من حماية نفسه من الاختراق عليه ألا يُشارك جُزافاً في أية معلومات، وأن يعرف الأشخاص الذين يتعامل معهم رقمياً،

يعمد "المهندس الاجتماعي" إلى مراقبة حسابات مواقع التواصل الاجتماعي للضحية، ويجمع عنه الكثير من المعلومات، ويدرس شخصيته ويعرف الكثير عنها رغم أنه لم يلتقيه، ومن ثم يصنع شخصية افتراضية ينتحلها ويتحدث إلى الضحية عبرها مستخدماً المعلومات التي جمعها عن حياته الشخصية بطريقة مدروسة، فيتقرب منه حتى يثق فيه، ثم يُملي عليه ما يريد للوصول إلى غاياته بسهولة، كأن يقنعه بالضغط على رابط مفخخ، أو بتحميل ملف يحتوي على برمجية خبيثة، أو ربما قد يخترق حاسوب الضحية ويستخدمه لنشر فيروس في أجهزة الشركة التي يعمل بها.

يُطوّر "المهندسون الاجتماعيون" بشكل مستمر أساليب جديدة لخداع ضحاياهم، فإلى جانب انتحال الشخصية، وخيانة الثقة التي يمنحها له الضحية والذي قد يكون صديقاً أو مقرباً، يعمد المخترقون إلى استغلال فضول الضحية وعواطفه وطباعه الشخصية، بالإضافة إلى استغلال المواضيع الجديدة والساخنة التي قد تكون محطّ اهتمام الكثيرين، للوصول لغاياتهم الاحتيالية.



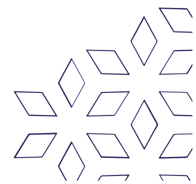
فكثيراً ما نصادف على وسائل التواصل الاجتماعي منشورات من قبيل "شارك المنشور مع ١٠ من أصدقائك لتدخل السحب على سيارة"، أو "اضغط على الصورة لتتحرك"، أو "املأ الاستمارة للدخول في سحب للفوز بجوائز قيّمة"، أو "حمّل ملف نسخة محدّثة عن تطبيق معين موثوق" بينما يكون الرابط خبيثًا، وبذلك تكون قد أهديت المخترق بياناتك الشخصية بكامل إرادتك، ليستخدم تلك المعلومات بسرقة حساباتك عن طريق تخمين كلمات السر، أو بيع تلك المعلومات إلى شركات المعلنين.

كما قد يعمد المخترق لاصطياد كلمة سر الضحية، من خلال إرسال صفحة من تصميمه تشبه صفحة تسجيل الدخول لأحد المواقع الشهيرة من حيث الشكل، لكنها تحمل عنواناً مختلفاً عن العنوان الأصلي، وعندما يُدخل الضحية كلمة السر للولوج إلى حسابه تصل بكل بساطة إلى المخترق ويكون الضحية قد وقع بالفخ دون أن يشعر بالخداع.

أما عن المعلومات التي قد يستهدفها المخترقون فهي تشمل كل ما يساعدهم في الحصول على الأموال، ورغم أنهم يركزون بشكل أساسي على الخدمات المالية كالحسابات البنكية وغيرها، إلا أنّ أي معلومة قد يتمكنون من الحصول عليها ستكون لها قيمة وتوظيف للوصول إلى غاياتهم. من الأمثلة على استخدام أساليب الهندسة الاجتماعية للاختراق ما حدث في الانتخابات الأمريكية الأخيرة التي جرت عام ٢٠١٦، إذ اتهم مكتب التحقيقات الفيدرالية "إف بي آي" الحكومة الروسية بالتدخل في الانتخابات الأمريكية، عبر اختراق تسبب في التلاعب بنتائج الانتخابات الرئاسية التي انتهت بفوز دونالد ترامب بالرئاسة على منافسته هيلاري كلينتون

وأظهرت التحقيقات أن مخترقين روس أنشؤوا آلاف الحسابات الوهمية على موقعي "فيس بوك" و "تويتر"، ليمرروا بواسطتها عددًا كبيرًا من الأخبار المضللة والشائعات، من خلال الدخول في نقاشات مع مواطنين أمريكيين وكسب ثقتهم.

كما كشفت شركة "غوغل"، أن عملاء روس أنفقوا عشرات الآلاف من الدولارات على نشر إعلانات على عدد من المواقع منها "يوتيوب"، و "جيميل"، ومحرك بحث "غوغل" وغيرها، في إطار حملة تضليل، مهمتها التأثير على نتائج الانتخابات الأمريكية.



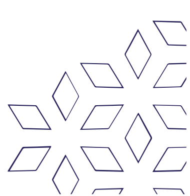
<u>كيف ننجو من الهجمات ونحمي أنفسنا من مخاطر الهندسة الاجتماعية؟</u>

ينصحنا الخبراء بـ:

- التثقيف في مجال الأمن الرقمي وأساليب الاختراق المتجددة.
- تجنب إعطاء أي معلومات سرية أو بيانات شخصية إلا بعد التأكد من هوية الشخص المتحدث، وأن الاتصال تمّ من جهة رسمية أو معروفة.
- تجنب الحديث في الأسرار الشخصية مع الأصدقاء المجهولين عبر وسائل التواصل الاجتماعي.
- عدم فتح ملفات أو مرفقات البريد الإلكتروني المُرسَل من أشخاص غير معروفين، والتأكد من الروابط المرسلة بأنّها ليست روابط خبيثة من خلال فتحها عبر استخدام موقع فيروس توتال.
- العمل على تأمين هواتفنا أو حواسيبنا واستخدام برامج لمكافحة الفيروسات.

❖ إجراءات الحد من مخاطر الهندسة الاجتماعية

بالإضافة إلى اكتشاف أي هجوم، يمكنك أيضاً أن تكون استباقياً بشأن خصوصيتك وأمانك، تعد معرفة كيفية منع هجمات الهندسة الاجتماعية أمراً مهماً للغاية لجميع مستخدمي الأجهزة المحمولة وأجهزة الكمبيوتر.



فيما يلي بعض الطرق المهمة للحماية من هجمات الهندسة الاجتماعية:

- **الاتصال الآمن وإدارة الحساب**

الاتصال عبر الإنترنت هو المكان الذي تكون فيه عرضة للخطر بشكل خاص حيث تعد وسائل التواصل الاجتماعي والبريد الإلكتروني والرسائل النصية أهدافاً شائعة ودائمة.

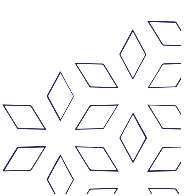
-لا تنقر أبداً على الروابط في أي رسائل بريد إلكتروني أو رسائل أخرى عبر وسائل التواصل الاجتماعي.

-استخدم المصادقة الثنائية، تعد الحسابات عبر الإنترنت أكثر أماناً عند استخدام أكثر من مجرد كلمة مرور لحمايتها، تضيف المصادقة الثنائية طبقات إضافية للتحقق من هويتك عند تسجيل الدخول إلى الحساب، يمكن أن تشمل عوامل المصادقة الثنائية القياسات الحيوية مثل بصمات الأصابع أو التعرف على الوجه، أو رموز المرور المؤقتة المرسلة عبر رسالة نصية.

–استخدم كلمات مرور قوية، يجب أن تكون كل كلمة مرورك فريدة ومعقدة مكونة من الأحرف الكبيرة والأرقام والرموز.

–تجنب مشاركة أسماء أشخاصك المهمين، أو حيواناتك الأليفة، أو مكان ميلادك، أو أي تفاصيل شخصية أخرى، قد تقوم بكشف إجابات لأسئلة الأمان الخاصة بك التي تستخدم في إعادة تعيين كلمة المرور (من هو صديق الطفولة؟) أو أجزاء من كلمة المرور الخاصة بك دون قصد، إذا أعددت أسئلة الأمان الخاصة بك بحيث لا تُنسى، ولكنها غير دقيقة بحيث يصعب تخمينها، فستجعل من الصعب على المجرم اختراق حسابك.

كن حذراً جداً في بناء صداقات عبر الإنترنت ووسائل التواصل الاجتماعي، على الرغم من أن الإنترنت يمكن أن يكون وسيلة رائعة للتواصل مع الأشخاص في جميع أنحاء العالم، إلا أن هذه طريقة شائعة لهجمات الهندسة الاجتماعية، راقب التحذيرات والإشارات والايحاءات المريبة التي تشير إلى التلاعب أو إساءة استخدام الثقة بشكل واضح.



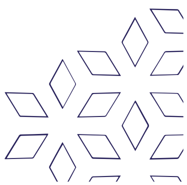
- **استخدام شبكة امنة للاتصال بالأنترنت**

يمكن أن تكون شبكات الإنترنت المُخترقة نقطة ضعف أخرى يتم استغلالها لاعتراض اتصالك والحصول على بيانات وصول لحساباتك، لتجنب ذلك، اتخذ إجراءات وقائية لأي شبكة تتصل بها.

لا تسمح أبداً للغرباء بالاتصال بشبكة Wi-Fi الأساسية. في المنزل أو في مكان العمل، يجب توفير اتصال Wi-Fi للضيوف، هذا يسمح لاتصالك الرئيسي المشفر والمؤمن بكلمة مرور أن يظل آمناً وخالياً من الاعتراض، إذا قرر شخص ما "التنصت على الشبكة من خلال اعتراض الاتصال" للحصول على معلومات، فلن يتمكن من الوصول إلى النشاط الذي ترغب أنت والآخرون في الحفاظ على خصوصيته،

استخدم VPNفي حالة اتصل شخص ما بشبكتك الرئيسية – سلكية أو لاسلكية أو حتى خلوية – لاعتراض حركة المرور على الشبكة، يمكن لشبكة افتراضية خاصة (VPN) حماية بياناتك، الشبكات الافتراضية الخاصة هي خدمات تمنحك "نفقًا" خاصاً ومشفّراً على أي اتصال إنترنت تستخدمه، اتصالك ليس فقط محمياً من الأعين غير المرغوب فيها، ولكن بياناتك ستكون مجهولة المصدر لذلك لا يمكن تتبعها.

حافظ على أمان جميع الأجهزة والخدمات المتصلة بالشبكة، كثير من الناس على دراية بممارسات أمان الإنترنت لأجهزة الكمبيوتر المحمولة والتقليدية. ومع ذلك، فإن تأمين شبكتك نفسها، بالإضافة إلى جميع أجهزتك الذكية والخدمات السحابية، لايقل أهمية عن ذلك، تأكد من حماية الأجهزة التي يتم التغاضي عنها بشكل شائع مثل أنظمة المعلومات والترفيه في السيارة وأجهزة توجيه الشبكة المنزلية، يمكن أن تؤدي انتهاكات البيانات على هذه الأجهزة إلى استخدامها في هجمات الهندسة الاجتماعية.



- **الحفظ على أمن جهازك**

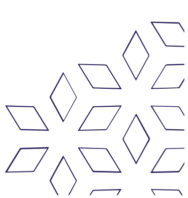
إن الحفاظ على أجهزتك نفسها لايقل أهمية عن جميع سلوكياتك الرقمية الأخرى، **احمي هاتفك المحمول وجهازك اللوحي وأجهزة الكمبيوتر من خلال:**

-استخدم برامج الأمان ففي حالة نجاح هجوم الهندسة الاجتماعية في اقناعك بتحميل برنامج ضار، ولمكافحتها والحماية منها عليك استخدام برامج مكافحة الفيروسات والبرامج الضارة للقضاء على كل مصادر الخطر.

–لاتترك أجهزتك غير آمنة في الأماكن العامة مطلقاً، قم دائماً بقفل جهاز الكمبيوتر والأجهزة المحمولة، خاصة في العمل، عند استخدام أجهزتك في الأماكن العامة مثل المطارات والمقاهي، احتفظ بها دائماً في حوزتك.

–حافظ على تحديث جميع برامجك بمجرد توفرها، توفر التحديثات الفورية لبرنامجك إصلاحات أمان أساسية عند تخطي أو تأخير التحديثات لنظام التشغيل أو التطبيقات، فإنك بذلك تترك ثغرات أمنية معروفة مكشوفة للمتسللين لاستهدافها، نظراً لأنهم يعرفون أن هذا سلوك العديد من مستخدمي الكمبيوتر والجوّال، فإنك تصبح هدفًا رئيسياً لهجمات البرامج الضارة.

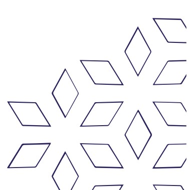
–تحقق من انتهاكات البيانات المعروفة لحساباتك عبر الإنترنت، ضع حسابات في خدمات مثل Kaspersky Security Cloud والتي تقوم بنشر ومتابعة عمليات اختراق البيانات الجديدة فإذا تم تضمين حساباتك في بيانات تم اختراقها، فستتلقى إشعاراً مع نصائح حول كيفية اتخاذ إجراء.



❖ طرق رئيسية لحماية الأجهزة والمعلومات من الإختراق

نظراً لما تحمله تلك الهجمات من خطورة بالغة سواء على مستوى الأفراد أو المؤسسات، وجب التحصين ضد هجمات الهندسة الاجتماعية، ومحاولة استخدام أي أدوات من أجل حفظ بياناتك أنت وأسرتك أو حتى شركتك من تلك القرصنة الخبيثة.

- عدم مشاركة بياناتك الشخصية مع أي شخص حتى وإن كان محل ثقة، وخاصة بياناتك البنكية.
- لاتضغط على أي روابط تصلك من أي شخص، حتى وإن كان صديقك المقرب –قد يكون حسابه اخترق بالفعل، وأنت الضحية القادمة.
- لاتضغط على أي ملفات تصلك عبر البريد الإلكتروني، فهي أشهر السبل المستخدمة عالمياً لنشر البرامج الخبيثة.
- استخدم تقنيات حديثة لترشيح رسائل البريد التي تصل إليك، حيث تؤدي تلك التقنيات وظيفة حارسك الشخصي، لترسل أي رسالة مرسلة من جهة مجهولة الهوية إلى ملف الرسائل المزعجة في البريد الإلكتروني.
- احرص على تثبيت برامج حماية من الفيروسات فعالة وذات سمعة طيبة، أو استعن بأحد الشركات المتخصصة في الأمن السيبراني لتساعدك على تلك المهمة.



سابعاً: الاصطياد والهجوم الالكتروني

في هذا الفصل سنتعرف على المواضيع التالية:

- نظام البريد الالكتروني
- الاصطياد الالكتروني
- التجسس الالكتروني
- مفهوم الهجوم الالكتروني
- أنواع الهجوم الالكتروني

❖ نظام البريد الالكتروني

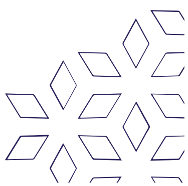
مكونات نظام البريد الالكتروني

ما هو عنوان البريد الإلكتروني؟

يشهد عالمنا اليوم ثورة كبيرة فيما يتعلق بمجال الاتصالات، خاصةً مع ظهور شبكة الإنترنت التي منحت الكثيرين إمكانية الدخول إليها وزيارة مواقعها وتحميل التطبيقات المختلفة من خلالها والتي تبقيك على تواصل دائم مع أحبتك وأصدقائك، إلى جانب استخدامها في مجال العمل، ومن الأمور التي تُمكّنك من الدخول إلى التطبيقات والمواقع المتاحة على الإنترنت هو البريد الإلكتروني، إذ عليك أن تنشئ حساباً مخصصاً لك لتتمكن من الدخول والاستفادة من هذه التطبيقات، ويُعرف عنوان البريد الإلكتروني؛ على أنه مُعرّف فريد لحسابات البريد الإلكتروني، والتي تُستخدم لإرسال واستقبال رسائل البريد الإلكتروني عبر الإنترنت، وكما هو الحال في البريد الفعلي، تتطلب رسالة البريد الإلكتروني عنواناً لكل من المرسل والمستقبل لتتمكن من إرسالها بنجاح.

أجزاء عنوان البريد الإلكتروني

يُستخدم البريد الإلكتروني كأداة اتصال بين الأفراد، وذلك من خلال إرسال واستقبال الرسائل بين المرسل والمستقبل، فعندما ترسل بريداً إلكترونياً إلى شخص ما، فأنت تنشئ رمزاً معيناً لاتستجيب له سوى خوادم الإنترنت، ويتكون عنوان البريد الإلكتروني النموذجي من ثلاثة مكونات، لكل منها دور وأهمية في عملية تبادل الرسائل، فإذا كان أحد هذه المكونات خاطئاً أو مفقوداً ستصلك رسالة خطأ أو سترسل رسالة البريد الإلكتروني إلى الجهة غير المقصودة بدلاً من ذلك، **وفيما يلي سنوضح لك المكونات الثلاثة الأساسية لعنوان البريد الإلكتروني:**

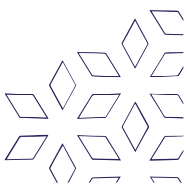


- **اسم المستخدم "Username":**

يُعد اسم المستخدم الجزء الأول من عنوان البريد الإلكتروني، وهو الاسم الفريد الذي تحدده أنت أو موفر خدمة الإنترنت، ويمكنك اختيار اسمك الحقيقي أو لقبك كاسم مستخدم لعنوان بريدك الإلكتروني، ومن الضروري أن يكون اسم المستخدم فريداً بمعنى أنه يجب ألا يكون لشخصين أو مؤسستين نفس اسم المستخدم مع نفس الموفر، وعند التسجيل للحصول على حساب بريد إلكتروني سواء أكان مجانياً أو مدفوعاً سيُطلب منك أولاً تحديد اسم مستخدم، ويُنصح بأن تختار اسم المستخدم الخاص بك بعناية خاصةً إذا كنت تخطط لاستخدام حساب بريدك الإلكتروني لإرسال رسائل بريد إلكتروني احترافية، وذلك لأن استخدامك لاسم مستعار أو مضحك مهما كان جذاباً إلا أنه غير مناسب لأصحاب العمل الذين سترسل إليهم سيرتك الذاتية بالبريد الإلكتروني في المستقبل.

- **رمز "@":**

يُعد الرمز "at" أو "@" الجزء الثاني من عنوان البريد الإلكتروني، والذي يقع بين اسم المستخدم ومجال عنوان بريدك الإلكتروني، وعندما تدخل الرمز، يتعرف برنامج البريد الإلكتروني الخاص بك على الحرف ويرسل البريد الإلكتروني إلى اسم المجال الذي يليه .



- **<u>اسم النطاق أو المجال:</u>**

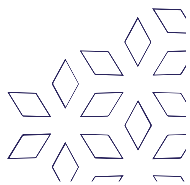
وهو الجزء الأخير من عنوان البريد الإلكتروني، والذي يمكن تقسيمه إلى جزأين هما؛ خادم البريد ونطاق المستوى الأعلى، ويُعرف خادم البريد بأنه المسؤول عن استضافة حساب البريد الإلكتروني، فعلى سبيل المثال تستخدم حسابات البريد الإلكتروني في شركة ياهو الاسم "Yahoo" كاسم الخادم، بينما يستخدم حساب الجيميل الاسم "Gmail" كاسم الخادم، بينما يُعرف نطاق المستوى الأعلى بالامتداد مثل؛ (com) أو (net) أو (info)، وغالباً ما تحتوي رسائل البريد الإلكتروني الواردة من المؤسسات التعليمية على الامتداد (edu)، بينما يستخدم موظفو الهيئات الحكومية الامتداد (gov).

الرسائل البريد الالكترونية غير المرغوبة

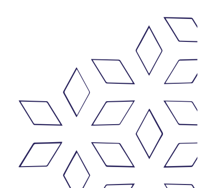
بالإنجليزية (Email spam) أو بالإنجليزية (junk email) حيث يتم إرسال الرسائل غير المرغوب فيها عن طريق البريد الإلكتروني.

العديد من رسائل البريد الإلكتروني غير المرغوب فيها ذات طابع تجاري، ولكن قد تحتوي أيضا على روابط مقنعة تبدو أنها لمواقع ويب مألوفة، ولكنها تؤدي في الواقع إلى مواقع ويب أو مواقع ويب تستضيف برامج ضارة، وقد تتضمن رسائل البريد الإلكتروني غير المرغوب فيها أيضا برامج ضارة مثل النصوص البرمجية أو مرفقات الملفات القابلة للتنفيذ الأخرى (أحصنة طروادة).

وقد نمى البريد المزعج بشكل مطرد منذ أوائل التسعينيات، وتستخدم شبكات بوتنت أجهزة الكمبيوتر المصابة بالفيروس، لإرسال حوالي ٨٠٪ من الرسائل المزعجة، وبما أن حساب الرسائل غير المرغوب فيها يتحملها في الغالب المتلقي، الإعلان المؤثر ويختلف الوضع القانوني للرسائل الاقتحامية من ولاية إلى أخرى.



في الولايات المتحدة، أعلن أن البريد المزعج قانوني من قبل قانون كان – سبام CAN-SPAM لعام ٢٠٠٣ بشرط أن تلتزم الرسالة بالقواعد التي يحددها القانون وإف تي سي FTC حاول مزودو خدمة الإنترنت إسترداد تكلفة الرسائل الاقتحامية من خلال دعاوى قضائية ضد مرسلي الرسائل غير المرغوب فيها، على الرغم من أنهم لم ينجحوا في جمع الأضرار وعلى الرغم من الفوز في المحكمة، يجمع مرسلو الرسائل غير المرغوب فيها عناوين البريد الإلكتروني من غرف الدردشة والمواقع الإلكترونية وقوائم العملاء ومجموعات الأخبار والفيروسات التي تحصد كتابة عناوين المستخدمين، كما يتم أحيانا بيع عناوين البريد الإلكتروني التي يتم جمعها إلى مرسلي الرسائل غير المرغوب فيها الآخرين، وكانت نسبة البريد الإلكتروني غير المرغوب فيه حوالي ٩٠٪ من رسائل البريد الإلكتروني المرسلة، في نهاية عام ٢٠١٤.

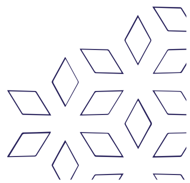


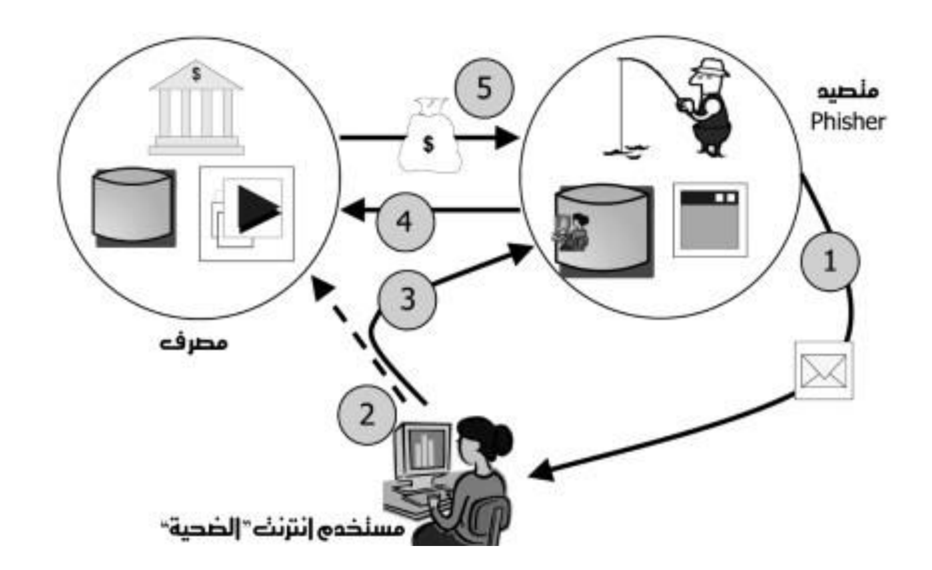
❖ الاصطياد الالكتروني

مفهوم الاصطياد الالكتروني وأماكن تواجده

الإصطياد الإلكتروني "phishing" هو نوع من هجمات الهندسة الاجتماعية للحصول على معلومات خاصة بمستخدمي الانترنت سواء كانت معلومات شخصية أو مالية عن طريق الرسائل الالكترونية أو مواقع الانترنت المزيفة.

وتتم هذه العملية عن طريق إرسال رسائل إلكترونية زائفة من قبل أشخاص يطلق عليهم المتصيدون phishers تطلب من الهدف أو الضحية بالنقر على رابط ضار، مما قد يؤدي إلى تثبيت برامج ضارة أو تجميد النظام كجزء من هجوم برامج الفدية أو الكشف عن معلومات حساسة، وقد يكون هذا الرابط هو عنوان لموقع انترنت مزيف صمم من قبل المتصيدون ويكون دائما شبيهاً بالموقع الأصلي، أما في ما يخص روابط الصفحات المزورة فهي تكون غالبا مكشوفة لأنه غير مطابق لرابط الموقع الأصلي و لهذا يلجأ بعض المتصيدون إلى قنص ضحايا عن طريق وضع روابط تشبه بشكل كبير الروابط الأصلية بحيث يكون الاختلاف بسيط جدا و يصعب على مبتدأ أو حتى شخص يعي هذه الأمور الإنتباه إلى أن هذا الرابط هو لصفحة مزورة، نأخذ موقع الفيس بوك كمثال فالكل يعلم أن رابط الموقع هو www.facebook.com يقوم المتصيد بإنشاء رابط يكون الاختلاف فيه بسيط جدا بحيث يكون رابط الصفحة المزورة مثلا www.facabook.com هنا قام المتصيد بتغيير حرف واحد فقط وهو حرف e ليصبح a وفي هذه الحالة يصعب على الضحية أن ينتبه إلى هذا الاختلاف خاصة إذا قام بفتح الرابط وظهرت له صفحة مشابهة تماما بالصفحة الأصلية للفيس بوك وبهذا يقوم الضحية بإدخال بياناته دون أن يعلم أنه تم الاطلاع على تلك البيانات المدخلة.





صورة توضح طريقة عمل الإصطياد الإلكتروني

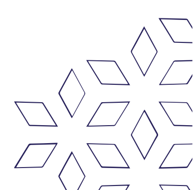
الإصطياد الإلكتروني لا يعتمد فقط على رسائل البريد الإلكتروني فقط فقد تطورت هذه العملية لتشمل تقنيات جديدة للوصول إلى الضحايا ومن أهم هذه التقنيات هي:

Redirection and Other Malicious Code-Based Schemes

وتعتمد هذه الطريقة على أن يقوم المستخدم عن غير معرفة بتحميل برامج خبيثة على حاسوبه حيث وظيفة هذه البرامج هي إعادة توجيه المستخدم من دون علمه إلى موقع شبيه تماما بالموقع الذي يريد الدخول إليه ويقوم المتصيد بجمع المعلومات الخاصة التي يدخلها المستخدم وتسمى هذه العملية Redirection إعادة التوجيه.

Vishing or voice phishing ويقصد بها التصيد الصوتي:

وتتم هذه العملية عن طريق إرسال رسالة إلى الضحية تحتوي على رقم هاتف مزيف لخدمة العملاء وعندما يقوم الضحية بالاتصال به يتم سؤاله عن معلومات الشخصية والمالية، أو أن يقوم المتصيد بالاتصال مباشرة بالضحية ويوهمه على أنه أحد موظفي خدمة العملاء، ومع استخدام تقنية الصوت عبر الإنترنت وبعض البرامج التي توحي للمستخدم بأن الرقم الذي اتصل به هو رقم مركز خدمة عملاء فعلي وبهذا يصعب على الضحية معرفة أنه واقع في مصيدة.

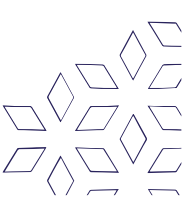


تصنيفات الاصطياد الالكتروني ودوافعه

أظهرت دراسات مختلفة تنوع الهجمات الإلكترونية في الأمن السيبراني، وكذلك وجود محاولات مستمرة من المجرمين الاكترونيين لتطوير أساليب الهجمات السيبرانية لتتوافق مع أي تحديثات أمنية يقوم بها خبراء الأمن السيبراني.

وفي هذا المقال سنذكر ٢٠ من أبرز أنواع الهجمات الإلكترونية شيوعاً والمكتشفة حتى عام ٢٠٢١ وهي كالآتي:





١. هجمات التصيد الاحتيالي(PHISHING ATTACKS)

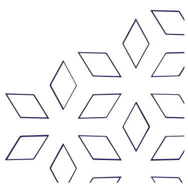
التصيد الاحتيالي هو نوع من هجمات الهندسة الاجتماعية يُستخدم غالباً لسرقة بيانات المستخدم، بما في ذلك بيانات اعتماد تسجيل الدخول وأرقام بطاقات الائتمان.

كيف يحدث هذا النوع من الهجمات السيبرانية؟

يبدأ هذا الهجوم عندما يتمكن المجرم الإلكتروني من خداع ضحية ما بعد تنكره على شكل كيان موثوق به، حيث يصل للضحية بريد إلكتروني أو رسالة نصية تحفزه على النقر فوق ارتباط ضار، وحالما يستجيب المستلم وينقر على الرابط يتم تثبيت برامج ضارة على جهازه أو تجميد النظام كجزء من هجوم برامج الفدية أو الكشف عن معلومات حساسة خاصة بالمستلم.

يمكن أن يكون لهذا النوع من الهجمات السيبرانية نتائج مدمرة بالنسبة للأفراد، يشمل ذلك عمليات الشراء غير المصرح بها أو سرقة الأموال أو سرقة الهوية، أما بالنسبة للمنظمات فغالباً ما يتم استخدام التصيد الاحتيالي للحصول على موطئ قدم في شبكات المنظمة أو الشبكات الحكومية كجزء من هجوم أكبر، مثل حدث التهديد المستمر المتقدم (APT) ، في هذه الحالة يتم اختراق الموظفين من أجل تجاوز الحدود الأمنية الخاصة بالمنظمة، أو توزيع البرامج الضارة داخل بيئة مغلقة، أو الحصول على تصريح للوصول إلى بيانات المنظمة الحساسة المحمية.

عادة ما تتكبد المنظمة التي تخضع لمثل هذا الهجوم خسائر مالية فادحة بالإضافة إلى انخفاض حصتها في السوق وفقدان سمعة وثقة عملائها، واعتماداً على نطاق هذا الهجوم من المحتمل أن تتصاعد محاولة التصيد الاحتيالي إلى حادث أمني للمنظمة يجعلها بموقف صعب قد لا تجد قدرة على التعافي منه.



٢. هجمات التصيد الاحتيالي بالرمح(SPEAR PHISHING)

التصيد بالرمح هو عملية احتيال تتم أيضاً عبر البريد الإلكتروني أو الاتصالات الإلكترونية، وتستهدف فرداً أو منظمة أو شركة معينة، على الرغم من أن مجرمي الإنترنت يسعون غالباً إلى سرقة البيانات لأغراض ضارة، إلا أنهم قد يعلمون أيضاً تثبيت برامج ضارة على جهاز كمبيوتر الضحية.

كيف يحدث هذا النوع من الهجمات السيبرانية؟

تصل رسالة بريد إلكتروني للضحية وتبدو بأنها من مصدر موثوق، ولكنها بدلاً من ذلك تقود المستلم إلى موقع ويب مزيف مليء بالبرامج الضارة، وغالباً ما تستخدم رسائل البريد الإلكتروني هذه تكتيكات ذكية لجذب انتباه الضحايا.

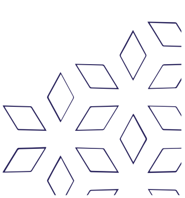
على سبيل المثال، حذر مكتب التحقيقات الفيدرالي (FBI) من عمليات التصيد بالرمح حيث كان يصل للضحايا رسائل بريد إلكتروني تبدو بأنها واردة من المركز الوطني للأطفال المفقودين والمستغلين لتبدو أنها كيان موثوق، وقد كانت تلك الرسائل مزيفة وتهدف لاختراق أجهزة مستلميها.

٣. هجمات تصيد الحيتان(WHALE PHISHING)

تصيد الحيتان هو مصطلح يستخدم لوصف هجوم التصيد الذي يستهدف بشكل خاص الوصول إلى معلومات حساسة وسرية لشخصيات قوية من الأفراد الأثرياء أو الأقوياء أو البارزين (على سبيل المثال، الرئيس التنفيذي لأي شركة) إذا أصبح فرد ما ضحية لهجوم تصيد احتيالي من هذا النوع، فيمكن اعتباره "تصيداً كبيراً" أو ما يسمى، "حوت".

ما علاقة هذا الهجوم بهجمات التصيد الاحتيالي؟

يعد صيد الحيتان في الأمن السيبراني مجموعة فرعية من هجمات التصيد الاحتيالي التي تستخدم طريقة استهداف محددة، تم إنشاؤها بواسطة مجرمي الإنترنت لانتحال شخصية عضو معين في شركة أو مؤسسة، حيث يستهدف المهاجمون الشركات المعنية لسرقة معلومات سرية أو إقناع الضحية بإرسال أموال أو بطاقات هدايا إلى المنتحل.



٤. هجماتDRIVE-BY

يشير هجوم Drive-by إلى هجوم إلكتروني يتسبب فيه برنامج نصي ضار في قيام برنامج ما بتنزيل وتثبيت نفسه على جهاز الضحية، دون إذن صريح منه.

يمكن أن يحدث هذا النوع من الهجمات السيبرانية على أي جهاز مستخدم يعمل بأي نظام تشغيل، وغالباً ما تحدث هذه الهجمات عندما ينتقل المستخدم إلى صفحة ويب تم اختراقها ويتصفحها،

تم تصميم هجمات Drive-by لإصابة الأجهزة أو سرقة المعلومات أو التسبب في تلف البيانات، والذي يستخدم غالباً مجموعات الاستغلال (Exploit kits) لبدء التنزيل التلقائي.

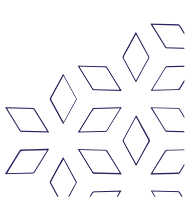
ما هيExploit kits ؟

هي أجزاء ضارة من البرامج، تم إنشاؤها بواسطة المتسللين لتحديد نقاط الضعف في جهاز أو مستعرض ويب أو تطبيق قائم على الويب، ثم يتم استخدام نقاط الضعف هذه لبدء عملية التنزيل التلقائي وتنفيذ الهجوم.

٥. برامج الفدية(RANSOMWARE)

تعتبر برامج الفدية أحد أكثر الهجمات السيبرانية خطورة في هذا العصر، والذي تمكن من جعل المعلومات الحساسة للأفراد والمنظمات على المحك.

في هذا النوع من الهجمات، يضطر الضحية إلى حذف جميع المعلومات الضرورية من نظامه إذا فشل في دفع فدية ضمن الجدول الزمني الذي قدمه مجرمو الإنترنت، حيث إنهم غالباً يبتزون المستخدم بنشر ملفاته الهامة بحال لم يتم دفع الفدية.



٦. الهجوم بكلمة المرور

في هذا النوع من الهجمات السيبرانية، يحاول المهاجمون اختراق حسابات مختلفة للضحايا من خلال اختراق ملفاتهم الشخصية وكلمات المرور الخاصة بهم مما يمنحهم وصولاً غير قانوني إلى جميع معلومات الضحية ليتم استخدامها من المهاجمين لتحقيق أهدافهم من سرقة البيانات أو التصيد الاحتيالي أو إدخال البرامج الضارة على الشبكات.

ويتحدث الخبراء بأنه على الرغم من سهولة وإمكانية التخفيف من هذه الهجمات، إلا أن العديد من المنظمات لا تطبق الضمانات وأساليب الحماية بشكل صحيح.

٧- هجمات التنصتEAVESDROPPING

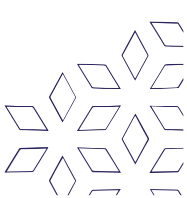
هجوم التنصت، المعروف أيضاً باسم هجوم sniffing أو التطفل snooping ، هو سرقة المعلومات حيث يتم نقلها عبر شبكة عن طريق جهاز كمبيوتر أو هاتف ذكي أو جهاز آخر متصل.

يستفيد هذا النوع من الهجمات السيبرانية من اتصالات الشبكة غير الآمنة للوصول إلى البيانات أثناء إرسالها أو استلامها من قبل مستخدمها عبر الشبكة لسرقتها.

كيف يمكن منع هذا النوع من الهجمات السيبرانية؟

يمكن منع هجمات التنصت بعدة طرق أبرزها:

- استخدام جدار حماية شخصي.
- الحفاظ على تحديث برامج مكافحة الفيروسات.
- واستخدام شبكة افتراضية خاصة(VPN) .
- تجنب شبكات wi-fi العامة.
- اعتماد كلمات مرور قوية.



٨- هجمات البرامج الضارة(MALWARE ATTACKS)

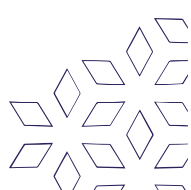
هجمات البرامج الضارة هي أي نوع من البرامج الضارة المصممة لإحداث ضرر أو تلف لجهاز كمبيوتر أو خادم أو عميل أو شبكة دون معرفة المستخدم النهائي.

ينشئ المهاجمون عبر الإنترنت البرامج الضارة ويستخدمونها ويبيعونها لأسباب عديدة مختلفة، ولكن غالباً ما يتم استخدامها لسرقة المعلومات الشخصية أو المالية أو التجارية، على الرغم من اختلاف دوافعهم، يركز المهاجمون الالكترونيون دائماً تكتيكاتهم وتقنياتهم وإجراءاتهم (TTP) على الوصول إلى بيانات الاعتماد والحسابات المميزة لتنفيذ مهمتهم.

٩- حصان طروادة(TROJAN HORSES)

وهو نوع من البرامج الضارة يتم إخفاؤه عادةً كمرفق في رسالة بريد إلكتروني أو ملف مجاني للتنزيل، ثم ينتقل إلى جهاز المستخدم، بمجرد التنزيل، سينفذ الكود الضار المهمة التي صممها المهاجم من أجلها، مثل الوصول إلى الباب الخلفي لأنظمة الشركة، أو التجسس على نشاط المستخدمين عبر الإنترنت، أو سرقة البيانات الحساسة.

تتضمن مؤشرات نشاط حصان طروادة على الجهاز نشاطاً غير عادي مثل تغيير إعدادات الكمبيوتر بشكل غير متوقع.



١٠- هجمات الرجل في الوسط(MAN-IN-THE-MIDDLE ATTACKS)

هجوم man-in-the-middle هو نوع من هجمات التنصت، حيث يقاطع المهاجمون محادثة موجودة أو نقل بيانات سرية بين طرفين.

كيف يحدث ذلك؟!

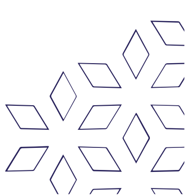
بعد تمكن المهاجمون من الدخول إلى "منتصف" النقل، يتظاهر المهاجمون بأنهم مشاركين شرعيين يمكّن هذا المهاجمين من اعتراض المعلومات والبيانات من أي طرف بهدف سرقة المعلومات السرية وإلحاق الضرر عبر إرسال روابط ضارة أو معلومات أخرى إلى كل من المشاركين الشرعيين الأساسيين بطريقة قد لا يتم اكتشافها إلا بعد فوات الأوان.

يوجد العديد من الاختصارات الشائعة لهجوم man-in-the-middle منها: MITM و MitM و MiM.

١١- هجمات رفض الخدمة (DOS: DENIAL-OF-SERVICE) وهجمات رفض الخدمة الموزعة (DDOS: DISTRIBUTED DENIAL-OF-SERVICE)

يؤدي هجوم رفض الخدمة (DoS) إلى إغراق الخادم بحركة المرور، مما يجعل موقع الويب أو المورد غير متاح. أما هجوم رفض الخدمة الموزع (DDoS) هو هجوم DoS يستخدم أجهزة كمبيوتر أو أجهزة متعددة لإغراق مورد مستهدف.

كلا النوعين من الهجمات يغمران الخادم أو تطبيق الويب بهدف مقاطعة الخدمات، ونظراً لأن الخادم يتم غمره بمزيد من حزم (TCP / UDP) أكثر مما يمكنه معالجتها، فقد يتعطل، وقد تتلف البيانات، وقد يتم توجيه الموارد بشكل خاطئ أو حتى استنفادها لدرجة شل النظام.



١٢- التلاعب بـURL (URL Manipulation)

لا تعد عناوين URL مجرد عناوين للمتصفحات والخوادم لاستخدامها أثناء انتقال المستخدمين من صفحة إلى أخرى باستخدام الروابط، فهي عبارة عن طلبات من المتصفح إلى الخادم والتي تعمل كشكل من أشكال البرمجة منخفضة المستوى، عندما يطلب المتصفح X من الخادم، يستجيب الخادم بـY .

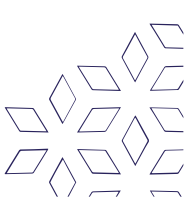
من الجدير بالذكر أنه لا يوجد ما يمنع المستخدمين من إدخال "أوامر" أخرى في شريط المتصفح لمعرفة ما سيعيده الخادم لهم.

يمكن للمتسلل من خلال التلاعب بأجزاء معينة من عنوان URL التحول لصفحات الويب التي لا يُفترض أن يكون لديه إمكانية الوصول إليها، يعد التلاعب في عنوان URL أحد أسهل الهجمات التي يتم إجراؤها، والذي يمكن أن يتم تنفيذها بواسطة مستخدمين فضوليين ببراءة أو متسللين يبحثون عن نقاط الضعف.

13- DNS TUNNELING

هو هجوم يصعب اكتشافه يقوم بتوجيه طلبات DNS إلى خادم المهاجم، مما يوفر للمهاجمين قناة قيادة وتحكم سرية ومسار لتصفية البيانات.

يستخدم المهاجمون نفق DNS للحصول على البيانات من خلال جدران الحماية، يعمل نفق DNS على ترميز رسائل الأوامر والتحكم (C&C) أو كميات صغيرة من البيانات إلى استجابات واستعلامات DNS غير واضحة، نظراً لأن رسائل DNS لا يمكن أن تحتوي إلا على كمية صغيرة من البيانات، يجب أن تكون أي أوامر صغيرة ويتم استخراج البيانات ببطء، يصعب اكتشاف هذه التقنية لأن DNS بروتوكول صاخب، مما يجعل من الصعب التمييز بين استعلام مضيف عادي وحركة مرور DNS العادية عن النشاط الضار.



١٤- اختطاف الجلسة SESSION HIJACKING

يعمل هجوم Session Hijacking على استغلال آلية التحكم في جلسة الويب، والتي تتم إدارتها عادةً لرمز مميز للجلسة.

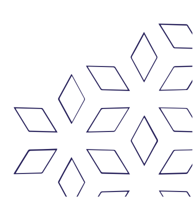
يتَّبع هذا النوع من الهجمات السيبرانية طريقة للاستيلاء على جلسة مستخدم الويب عن طريق الحصول خلسة على معرف الجلسة والتنكر في صورة المستخدم المصرح له.

بمجرد الوصول إلى معرف جلسة المستخدم، يمكن للمهاجم أن يتنكر مثل هذا المستخدم ويفعل أي شيء مخول للمستخدم القيام به على الشبكة.

١٥- القوة الغاشمة (BRUTE FORCE)

يعل المهاجمون في هذا النوع من الهجمات السيبرانية على تجربة مجموعات مختلفة من أسماء المستخدمين وكلمات المرور حتى يعثروا على واحدة تعمل، وقد يعمل المهاجم على تخمين المفتاح الذي يتم إنشاؤه عادةً من كلمة المرور باستخدام وظيفة اشتقاق المفتاح (key derivation function) ويُعرف هذا بالبحث الشامل عن مفتاح.

يوصي الخبراء بالعمل على تصيد هجوم القوة الغاشمة وتحييده فبمجرد وصول المهاجمين إلى الشبكة، سيكون القبض عليهم أكثر صعوبة.



١٦- هجمات البرمجة النصية عبر المواقع(CROSS-SITE SCRIPTING)

هجمات البرمجة النصية عبر المواقع (XSS) هي نوع من الحقن، حيث يتم حقن البرامج النصية الخبيثة في مواقع الويب الحميدة والموثوقة.

تحدث هجمات XSS عندما يستخدم المهاجم تطبيق ويب لإرسال تعليمات برمجية ضارة، بشكل عام في شكل نص برمجي من جانب المستعرض، إلى مستخدم نهائي مختلف. لا بد من العمل بشكل دائم على اكتشاف العيوب التي قد تسمح لهذه الهجمات بالنجاح، حيث إنه من الممكن أن تحدث في أي مكان يستخدم فيه تطبيق الويب مدخلات من المستخدم ويعمل على معالجتها وتوليد المخرجات بشكل مباشر لها دون التحقق من صحتها أو تشفيرها.

١٧- حقن SQL (SQL INJECTION)

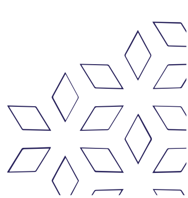
يتكون هجوم حقن SQL من إدخال أو "حقن" استعلام SQL عبر حقول الإدخال من العميل إلى التطبيق من أجل التأثير على تنفيذ أوامر SQL المحددة مسبقاً.

يمكن للمهاجم الذي يستخدم هذه الطريقة بحال نجاحها قراءة البيانات الحساسة من قاعدة البيانات، وتعديل بيانات قاعدة البيانات من (إدراج / تحديث / حذف)، وتنفيذ عمليات الإدارة على قاعدة البيانات (مثل إيقاف تشغيل DBMS)، واستعادة محتوى ملف معين موجود في DBMS وفي بعض الحالات إصدار أوامر لنظام التشغيل.

١٨- التهديدات من الداخل

تحدث العديد من أنواع الهجمات السيبرانية يومياً، والحقيقة الأكثر إثارة للصدمة هي أنه في معظم الأحيان، يكون هناك شخص من الداخل يشارك في العملية لمساعدة مجرمي الإنترنت في الحصول على معلومات حول منظمتهم، ويتم ذلك من خلال تزويد أولئك المجرمين بكل المعلومات الضرورية للولوج، مما يؤدي إلى عواقب كارثية على المنظمة.

تعتبر التهديدات من الداخل أحد التهديدات الشائعة للهجمات السيبرانية على البنوك والمؤسسات المالية.



١٩- هجمات الذكاء الاصطناعي

يركز التعلم الآلي على تعليم الكمبيوتر لأداء عدة مهام بمفرده بدلاً من الاعتماد على البشر في إجرائها يدوياً، يستخدم الذكاء الاصطناعي، في بعض الأحيان، لاختراق الأنظمة الرقمية للحصول على معلومات غير مصرح بها، كما يمكن استخدامه أيضاً لسرقة البيانات المالية السرية.

٢٠- هجمات عيد الميلاد(BIRTHDAY ATTACKS)

هجمات عيد الميلاد هي من أنواع القوة الغاشمة من الهجمات السيبرانية التي تهدف إلى تشويه الاتصال بين العملاء ومختلف الأفراد في الشركة بدءاً من المدير التنفيذي وانتهاء بموظفيها.

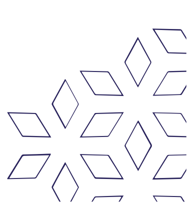
هجوم عيد الميلاد هو نوع هجوم التشفير الذي يكسر خوارزميات الرياضيات من خلال إيجاد التطابقات في دالة التجزئة.

تعتمد الطريقة على نظرية عيد الميلاد التي من خلالها تكون فرصة مشاركة شخصين في عيد ميلاد واحد أعلى بكثير مما تبدو عليه، وبنفس الطريقة، فإن فرصة اكتشاف التعارضات أعلى أيضاً ضمن وظيفة التجزئة المستهدفة، وبالتالي تمكن المهاجم من العثور على أجزاء مماثلة من خلال استخدام عدد قليل من التكرارات.

الإجراءات المضادة الاصطياد الالكتروني

توجد العديد من الإجراءات والطرق المضادة التي يمكن اتباعها لصد هجمات الاصطياد الالكتروني، حيث يمكن اتخاذ إجراءات من شأنها تحسين مقاومة هجمات الاصطياد الالكتروني قبل وقوعها، وتقليل الخسائر التي قد تنتج عنها، **وتندرج هذه الأنشطة بشكل رئيسي تحت الإجراءات التالية:**

١. منع هجمات الاصطياد الالكتروني قبل حدوثها (من خلال إنشاء بريد الكتروني للبلاغات ومراقبة كل من: رسائل البريد الالكتروني المرتدة، الصور التي تستخدم شعار المنظمة، حسابات العملاء)
٢. التصفية (Filteration)
٣. التحديثات الأمنية (Security Patches) وجدران الحماية (Firewall)
٤. تصفية الأكواد البرمجية الخبيثة (Cross-Site Script - XSS)
٥. لوحة المفاتيح المرئية (Visual Keyboard)
٦. التصديق الثنائي (Two-Factor Authentication)
٧. التصديق المتبادل (Mutual Authentication)
٨. أشرطة أدوات مكافحة الاصطياد الالكتروني (Anti-Phishing Toolbars)
٩. برامج مكافحة الاصطياد الالكتروني (Anti-Phishing Software)



❖ التجسس الالكتروني

تعريف التجسس الإلكتروني

التجسس الإلكتروني هو عبارة عن عدة طرق تتمركز على التقنية التكنولوجية والبرمجية للحصول على معلومات غير معلنة على العلن.

أكثر الاسلاك التي تعاني من التجسس الالكتروني هي الأسلاك الأمنية وكل ما يتعلق بها، خاصة وان العالم يعيش في حالة تنافسية لا تنتهي بين الدول العظمى وبين دول الصراع في الشرق الأوسط

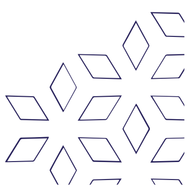
ويقوم بهذا النوع من الاختراقات المحوسبة مجموعات من المبرمجين الذين يكون هدفهم الأساسي هو الحصول على المعلومات اما عن طريق جهة رسمية او عن طريق اشخاص عابثين لا يملكون هدفاً واضحاً من التجسس بقدر ما يمارسون التجسس لتنمية مهاراتهم التجسسية عبر المنصات الالكترونية ومواقع التواصل الاجتماعي.

يتم التجسس عن طريق الوصول الى الملفات الرئيسية في الحواسيب والأجهزة الذكية وزرع برامج تجسس وتسجيل بيانات ثم رفعها الى أجهزة الشخص القائم بأعمال الابتزاز وحفظها في ملفات خاصة ليتم استخدامها في الوقت المناسب.

أهداف التجسس الإلكتروني

للتجسس الالكتروني عدة مهام وهي:

- **تجسس الهجوم:** ينفذ من أجل التجسس على العدو من خلال اختراق منظومة حواسيبه ومواقعه الإلكترونية ومهاجمة شبكات العدو بالفيروسات والتخريب وتدمير منظوماته الإلكترونية وهذه من أكثر طرق التجسس اتباعا بين الأطراف التي ينشب بينها صراع سياسي.
- **تجسس الرقابة:** هذا الأسلوب تقوم به الدول في غالب الأحيان من خلال مراقبة وسائل التواصل الاجتماعي ومراقبة حركة الأموال ومراقبة إيميلات وحواسيب المشتبه بهم وحتى مراقبة حركة عجلات الشرطة والجيش ضمن منظومة GPS .
- **تجسس الوقاية:** لصد تجسس العدو وتحصين شبكة حواسيب الدولة والأجهزة الأمنية لحماية الشبكات من الفيروسات وأي محاولات تخريبية ويتمثل ذلك بالتحول الرقمي وهذا النوع بالذات يأتي ردا على النوع الأول أي نوع التجسس الهجومي.



أشهر أساليب وطرق التجسس الإلكتروني

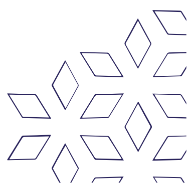
يمكن للتجسس ان يحدث بأكثر من طريقة وأسلوب، ولكن ما هي أكثر الطرق تطورا في المجال على ارض الواقع وكيف تعمل:

- **ساعة حائط:**

من أشهر أساليب التجسس هي ساعة الحائط حيث تحتوي على كاميرا مخفية وتعمل بتقنية G٣، مزودة ببطارية ذات عمر طويل. يمكن الاتصال بها عبر شريحة مزودة بها والاستماع إلى التسجيلات، كما يمكن أن تستقبل رسائل نصية لتفعيل عملها وبدء التسجيل أو الإيقاف، وبها إمكانية التسجيل بشكل مباشر إلى ذاكرة تخزين SD ويمكن وضع ذاكرة بحجم ٣٢ جيجا بايت. إضافة الى انه من الممكن بث تسجيل مباشر واستقباله بواسطة هاتف android ومتابعة ما يجري. هناك الكثير من هذه الأجهزة مثل أجهزة على شكل قلم أو ساعة يد أو ميدالية مفتاح سيارة شبيهة بجهاز الريموت للسيارات وغيرها وهي الأجهزة المتعارف عليها في الجاسوسية التقليدية، ولكنها تطورت فيما بعد لتصبح أحد اقوى أدوات التجسس الالكترونية.

- **أقمار التجسس التي تحتل السماء:**

تعتبر الأقمار الصناعية من اهم أساليب التجسس الالكتروني حيث انها تتطور كل عام مع تطور التكنولوجيا في العالم، يوجد ٥٠٠٠ قمر صناعي في سماء العالم وظيفتها مراقبة الدولة لسكانها ومراقبة الدول الأخرى التي من شأنها ان تحدث صراعات بينهما، غالبية الدول تصرح بأن اقمارها الصناعية هي أقمار مدنية وليست جاسوسية، ولكن التنافس على شراء هذه الأقمار والفائدة التي تعود إليهم منها تثبت عكس كلامهم المحكي.



- **تطبيقات الجاسوسية الالكترونية:**

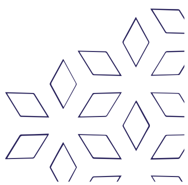
يستخدم هذا الأسلوب بالاعتماد على التنقل الجغرافي للشخص مع الربط على مواقع التواصل الاجتماعي ومتابعة المنشورات التي يقوم الشخص بنشرها والتفاعل معها، استخدمت هذه التطبيقات والبرامج مع الإرهابيين في دول العالم، الذين كانوا ينتمون الى جهات مشكوك بأمرها، يقوم البرنامج بمراقبة نشاط الفرد على المنصات الالكترونية وتتبع انتقاله وتسجيل الجهات التي يلتقي معها على ارض الواقع مع تسجيل صوتي للحديث الذي يدور بين هؤلاء الأطراف.

- **نظارات التجسس الاستخباراتية:**

تعتبر هذه النظارات أداة تجسس حكومي اذ يشتهر بها رجال الشرطة في الموانئ والمطارات، وهي عبارة عن نظارة شمسية تعطي الملف الجنائي الكامل لأي أحد يقع نظر الشرطي عليه، هذه النظارات وظيفتها الإمساك بالمجرم والتعرف عليه، حتى لو كان بين عشرات الالاف من الناس.

- **الحشرات التجسسية:**

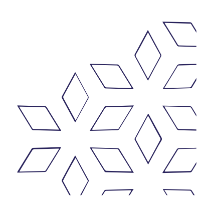
اليعسوف والصرصار والذبابة هم ٣ أنواع حشرات تم تطوير أجهزة تجسس تشبههم تماما ولكل واحد منهم تقنيات ومميزات تختلف عن الاخر، تم تطوير هذه الأجهزة في سنوات مختلفة ولكل منهم لوظيفة، اهم ووظيفة وأكثرها حساسية هي التي تملكها ذبابة التجسس وهي ان تحط على جسد الشخص المطلوب بمساعدة أجهزة الاستشعار والكاميرات الدقيقة وبعد ان تحط على جسده تقوم بسحب عينة حمض نووي من الشخص وحملها الى المركز المختص دون ان يشعر الشخص.



كانت تكمن أهمية أجهزة التجسس فقط فيما يخص الحياة السياسية والعسكرية، فالأدوات كانت تتوجد لأجل هذه الأهداف وتتطور فيما بعد حسب تطور الإمكانيات، ولكن اليوم أجهزة التجسس صارت أكثر دقة وأكثر اختراقا للخصوصية وللمجال الفكري، حتى ان فكرة "الكوكيز" صنفها الخبراء على انها أحد أدوات التجسس التجاري،

حيث انه يتم تفعيل كافة أجهزة وأنظمة الحسابات الالكترونية على توظيف إعلانات تتوافق مع الكلام الذي تقوله، والذي لا يعرفه الكثيرين ان لكل شخص داتا كاملة لدى شركة جوجل، وهي مساحة تخزين معلومات تسجل كافة التعليقات والتفاعلات والرسائل وبصمة الصوت والعين، كما انها تسمح للجهاز بأن يسجل صوتك ويتعرف على بصمته حتى وان كنت تتحدث على بعد ٣٠ متر من الجهاز.

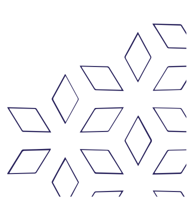
تنوع اهداف التجسس الالكتروني بما يتوافق مع العائد الربحي لكل من الشركات يجعلنا نفكر أكثر بالخطوات التي يجب ان نقوم بها لنحمي أنفسنا من التجسس الالكتروني بكافة حالاته..



كيف نحمي أنفسنا من التجسس الالكتروني؟

وفيما يلي أهم طرق مكافحة التجسس الالكتروني:

- المواظبة على عدم تفعيل تقنية التتبع الجغرافي داخل اجهزتك الذكية ومنصات وتطبيق العالم الرقمي، أي ان تشغل التعرف على موقعك الجغرافي مرة واحدة عندما تطلب انت وليس دائما ودون اذن.
- لا تتواصل مع جهات غير معروفة عبر مواقع التواصل الاجتماعي: تواصلك مع الأشخاص غير المعروفين يقرب منك الشكوك الأمنية والاستخباراتية وتبدأ عمليات التجسس ودراسة شخصيتك وانتماءاتك السياسية.
- لا تفعل نظام الكوكيز في الاستخدامات المحوسبة وواظب على اختيار التطبيقات الأقل تعاملا مع الإعلانات لكي لا تتحول أوقات تفاعلك مع العالم الرقمي الى أوقات عرض إعلانات وتحويلك الى مجرد الة استهلاك اقتصادية.
- لا تقم بضغط زر المتابعة او الإعجاب لأي صفحة تملك محتوى قد يصنف خطير او ينافي المعايير العامة وان كنت مصر على متابعة هذه الصفحات قم بدراسة كافة تفاعلاتك معها قبل ان تنفذها.
- استخدم كلمات مرور سرية ومكونة من أحرف لاتينية بعدة احجام وبعدم ترتيب هجائي إضافة الى الأرقام، وابتعد ابتعادا تاما عن التواريخ المعروفة لدائرتك الاجتماعية والكلمات المفتاحية السهلة، واربط كافة المواقع برقم هاتفك لضمان سريتك وتبليغك حول أي محاولة اختراق تحدث لأجهزتك الذكية.
- حمل التطبيقات الموثوقة لحماية بياناتك وموقعك الجغرافي وكافة محادثاتك واهتماماتك عبر مواقع التواصل الاجتماعي، مثل تطبيق نوي الحديث الذي يوفر حماية كاملة لكافة محتواك الالكتروني والمخزن على اجهزتك الذكية.



❖ مفهوم الهجوم الإلكتروني

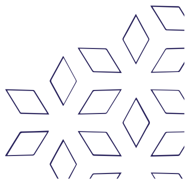
ما هو الهجوم الالكتروني، تحتل الهجمات الإلكترونية المرتبة الخامسة في قائمة المخاطر العالمية في عام ٢٠٢٠ وأصبحت قاعدة جديدة في القطاعين العام والخاص، وتستمر هذه الصناعة عالية المخاطر في النمو في عام ٢٠٢١، إذ من المتوقع أن تتضاعف الهجمات الإلكترونية عبر إنترنت الأشياء وحدها بحلول عام ٢٠٢٥، وسوف يتحدث موقع مقالاتي عبر هذا المقال عن تعريف الهجوم الإلكتروني، بشيءٍ من التفصيل.

من أين تأتي الهجمات الإلكترونية

العديد من الهجمات الإلكترونية انتهازية، إذ يكتشف المتسللون نقاط الضعف في دفاعات نظام الكمبيوتر ويستغلونها، وقد يتضمن ذلك العثور على عيوب في رمز موقع الويب، مما يسمح لهم بإدخال الكود الخاص بهم ثم تجاوز عمليات الأمان أو المصادقة، وقد يعني ذلك أيضاً قيامهم بتثبيت برامج ضارة وهي برامج مصممة خصيصاً لإتلاف نظام عبر موقع طرف ثالث ضعيف، ويُعدُّ مصدر الهجمات الإلكترونية من خلال أخطاء عادية مثل اختيار المستخدم لكلمة مرور سهلة التخمين، أو عدم تغيير كلمة المرور الافتراضية على شيء مثل جهاز التوجيه، يعد التصيد الاحتيالي طريقة شائعة للوصول إلى النظام، وهذا يتضمن استخراج المعلومات الشخصية بحجج خادعة.

ما هو الهجوم الالكتروني

ويطلق على الهجوم الإلكتروني اسم الهجوم السيبراني، ويُعرّف بأنهُ محاولة من قبل فرد أو مجموعة لتهديد نظام كمبيوتر أو شبكة أو جهاز، بقصد التسبب في ضرر معين، ومن الممكن أن تكون هذه الهجمات ضد الحكومات أو الشركات أو الأفراد وليست بالضرورة واسعة النطاق، وتشير بعض الدراسات أنّه يمكن للهجوم الإلكتروني أن يشل نظام الكمبيوتر بالكامل، مما يعني أن الشركة تخسر المال لأن موقعها على الويب لا يمكن الوصول إليه، أو يمكن أن تمنع هيئة حكومية من تقديم خدمة أساسية، وقد يؤدي إلى سرقة كميات كبيرة من البيانات الحساسة، والتي يمكن أن تؤثر بعد ذلك على الأفراد على المستوى الشخصي أو المالي، وفي بعض الحالات يمكن أن يتسبب ذلك في أضرار مادية كما حدث في عام ٢٠١٥ عندما تم اختراق مصنع للصلب في ألمانيا.



❖ أنواع الهجوم الإلكتروني

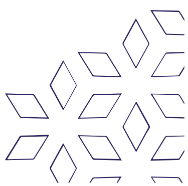
الهجوم الإلكتروني هو هجوم عبر الإنترنت ومحاولة من قبل مجرمي الإنترنت وقراصنة الكمبيوتر أو الخصوم الرقمية الأخرى للوصول إلى شبكة الكمبيوتر أو النظام، وعادة تكون لأغراض تغيير، وسرقة، وتدمير أو تعريض المعلومات للخطر، ويمكن أن تستهدف الهجمات الإلكترونية مجموعة واسعة من الضحايا من المستخدمين من الأفراد إلى الشركات أو حتى الحكومات، وعند استهداف الشركات أو المؤسسات الأخرى يكون هدف المتسلل الأساسي هو الوصول إلى موارد الشركة الحساسة والقيمة، مثل الملكية الفكرية، أو بيانات العملاء أو تفاصيل الدفع، وأبرز أنواع الهجمات الإلكتروني ما يأتي:

هجوم تعطيل الخدمة

يعمل هجوم رفض الخدمة على إغراق الأنظمة أو الخوادم أو الشبكات بسيل من حركة مرور البيانات لاستنفاد الموارد والنطاق الترددي، ونتيجة لذلك، يتعذر على النظام تنفيذ الطلبات المشروعة، كما يمكن للمهاجمين استخدام العديد من الأجهزة المخترقة لشن هذا الهجوم، ويُعرف هذا بهجوم رفض الخدمة الموزّع DDoS.

هجوم اختطاف البروتوكول

هو هجوم يتم فيه الاستيلاء على جلسة المستخدم من قبل المهاجم، ومن المتعارف ان الجلسة تبدأ عند قيامك بتسجيل الدخول إلى إحدى المواقع او الخدمات، على سبيل المثال المواقع المصرفية او المتاجر، وتنتهي الجلسة عند تسجيل الخروج وبالتالي يتم الاستلاء على هذه الجلسة والتصرف بها كأنه مالك الجلسة الفعلي.

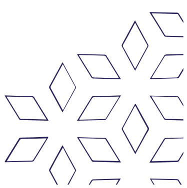


مراحل اختطاف الجلسة:

- **الاستطلاع:** تتضمن الخطوة الأولى في عملية اختطاف الجلسة قيام المهاجم بتحديد هدفه من أجل العثور على جلسة نشطة عادة، يستخدم المهاجمون تطبيقات مثل Sniffing Tools لمساعدتهم على إنجاز هذه الخطوة.
- **مراقبة الشبكة:** في هذه الخطوة، سيختبئ المهاجم في الشبكة المخترقة، محاولًا تحديد استخدام أي حركة مرور ضعيفة لم يتم تأمينها بشكل صحيح. من المعروف أن البروتوكولات مثل FTP و HTTPغير آمنة.
- **تحديد معرف الجلسة**: Session ID يستخدم المهاجم جميع المعلومات التي جمعها من خلال الخطوتين السابقتين لمحاولة التنبؤ ومعرفة ما هو رقم التسلسل للجلسة القادمة.
- **التسلل:** بعدما يتمكن المهاجم من معرفة رقم الجلسة القادمة الصحيحة، يقوم بالتسلل إلى الشبكة والاستيلاء على جلسة المستخدم أو الاستيلاء عليها بشكل كامل دون معرفة الشخص بذلك.

انواع الاختطاف:

- **الاختطاف النشط:** يتم فيه الاستلاء على الجلسة والتصرف بها كيفما يشاء المهاجم
- **الاختطاف الغير نشط:** يتم فيه اختطاف الجلسة دون التفاعل مع الضحية، بل يكتفى بالتجسس وتدوين الملاحظات.



هجمات البرامج أو الأكواد الخبيثة

البرامج الضارة هو مصطلح لوصف البرمجيات الخبيثة، بما في ذلك برامج التجسس spyware وبرامج الفدية الضارة والفيروسات وكذلك الفيروسات المتنقلة، تحاول البرامج الضارة اختراق الشبكة من خلال استغلال الثغرات الأمنية، ويتم ذلك عادةً عندما ينقر مستخدم ما على رابط خطير أو مرفق بريد إلكتروني يعمل على تثبيت البرامج الخطرة، وبمجرد الوصول إلى النظام، **يمكن للبرامج الضارة تنفيذ الآتي:**

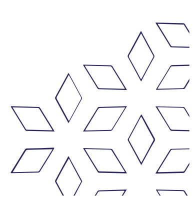
- حجب الوصول إلى المكونات الرئيسية للشبكة (برامج الفدية الضارة).
- تثبيت البرامج الضارة أو غيرها من البرامج المؤذية.
- الحصول على المعلومات بشكل خفي من خلال نقل البيانات من محرك الأقراص الثابتة (برامج التجسس).
- تعطيل مكونات محددة وجعل النظام غير صالح للعمل.

هجمات الهندسة الاجتماعية

الهندسة الاجتماعية هي محتوى يخدع الزائرين لحثهم على تنفيذ إجراءات خطيرة، مثل الكشف عن معلومات سرية أو تنزيل البرامج، إذا اكتشف محرك البحث Google أنّ موقعك الإلكتروني يتضمّن محتوى هندسة اجتماعية، قد يعرض متصفّح Chrome التحذير "أنت بصدد الانتقال إلى موقع إلكتروني مخادع" عندما يحاول الزائرون الدخول إلى موقعك الإلكتروني، يمكنك الانتقال إلى تقرير " مشاكل الأمان " للتحقق مما إذا كانت هناك أي صفحات على موقعك الإلكتروني يُشتبه في احتوائها على هجمات الهندسة الاجتماعية.

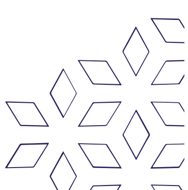
ما هي الهندسة الاجتماعية؟

تحدث هجمات الهندسة الاجتماعية عندما يتمّ خداع مستخدم الويب وحثّه على تنفيذ بعض الإجراءات الخطيرة على الإنترنت.



هناك أنواع مختلفة من هجمات الهندسة الاجتماعية:

- **التصيّد الاحتيالي:** يخدع الموقع الإلكتروني المستخدمين لحثهم على الكشف عن معلوماتهم الشخصية (على سبيل المثال، كلمات المرور أو أرقام الهواتف أو أرقام التأمين الاجتماعي). في هذه الحالة، يدّعي المحتوى من خلال التصميم والمظهر أو الوظيفة أنّه جهة موثوق بها، مثل متصفّح، أو نظام تشغيل ،أو مصرف أو حكومة.
- **المحتوى المخادع:** يحاول المحتوى خداعك وحثّك على تنفيذ إجراءات لا تجريها عادةً إلا مع جهة موثوق بها، مثل مشاركة كلمة مرور أو الاتصال بفريق الدعم الفني أو تنزيل برامج، أو أنّ المحتوى يشتمل على إعلان يدّعي كذباً أنّ برنامج الجهاز قديم، ويحث المستخدمين على تثبيت برنامج غير مرغوب فيه.
- **خدمات خارجية غير مكتملة التصنيف:** الخدمة الخارجية هي شخص يدير موقعاً إلكترونياً أو خدمةً بالنيابة عن جهة أخرى. إذا كنت (طرفاً ثالثًا) تدير موقعًا إلكترونياً بالنيابة عن طرف أخر (أول) بدون أن توضّح هذه العلاقة، قد يتم الإبلاغ عن هذا السلوك باعتباره هندسة اجتماعية، على سبيل المثال، إذا كنت (الطرف الأول) تدير موقعاً إلكترونياً خيرياً يستخدم موقعًا إلكترونياً لإدارة التبرعات (الطرف الثالث) يتولّى جمع التبرعات لموقعك الإلكتروني، يجب أن يحدّد موقع إدارة التبرعات بوضوح أنه منصة خارجية تتصرف بالنيابة عن الموقع الإلكتروني الخيري، وإلّا يمكن اعتباره من مواقع الهندسة الاجتماعية.



ثامناً: أمن التعاملات الالكترونية

في هذا الفصل سنتعرف على المواضيع التالية:

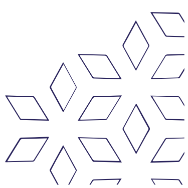
- مفهوم التصفح الآمن ومميزاته
- المخاطر التي تهدد المستخدم أثناء تصفح الإنترنت
- خطوات التصفح الأمن من خلال الإنترنت
- السياسيات الأمنية في المؤسسات الصحية
- الأمان في مواقع التواصل الاجتماعي
- حماية البيانات الشخصية في التجارة الالكترونية
- التحقق الرقمي من الهوية

❖ مفهوم التصفح الأمن ومميزاته

تعريف التصفح الآمن لشبكة الإنترنت يُعرف التصفح الآمن بالإنجليزية Safe Browsing : بأنّه أحد الخدمات التي أطلَقها فريق الأمان الخاص بِشركة جوجل العالمية (Google's security team)، وذلك بهدف تحديد مواقع الويب غير الآمنة عند تصفح الإنترنت وتنبيه المستخدمين وأصحاب تلك المواقع بالمخاطر المُتوقعة،إذ يَسمح التصفح الآمن بالتأكد من عناوين المواقع ومقارنتها مع قوائم جوجل المحدثّة والتي تَحتوي على مواقع الويب غير الآمِنة، وتشمل مواقع الويب غير الآمِنة؛ المواقع التي تحتوي على برامج ضارة غير مرغوب بها؛ كالفيروسات، أو مواقع الاحتيال والنصب.

يُعد التصفح الآمن ظاهرة تدعمُها مُتصفحات الإنترنت المختلفة وشركات التكنولوجيا لِحماية مُستخدِميها، وتُدرج جميع المواقع الضّارة في قاعدة بيانات واحدة تسمى القائمة السوداء، ويُمكن عندها للمُتصفحات مُقارنة مُحتويات القائمة السوداء مع موقع الويب لتحديد ما إذا كان الموقع آمناً أم لا، ومن المُتصفحات المعروفة والتي تَستخدم التصفح الآمن لِحماية مُستخدميها كل من؛ جوجل كروم (Google Chrome)، وسفاري (Safari)، وفايرفوكس (Firefox).

تُوفر بعض مُتصفحات الويب موارد محددة للتصفح بشكل آمن مثل؛ المتصفحMozilla Firefox ، والذي يُقدم مُكونات إضافية وخيارات خصوصية لِزيادة أمان التصفح مثل؛ Noscript وAdblock Plus، كما يُعد مُتصفح جوجل كروم بِحد ذاته مُتصفح آمن يُظهر تحذيرات المواقع المشبوهة والتي يُمكن أن تُسبب تهديد أو أي مشاكل في الأمن السيبراني، ويمكن تثبيت متصفح جوجل كروم للاستفادة من خصائصه المتعلقة بالتصفح الآمن، بالإضافة إلى ذلك تُقدم مَنصات التواصل الاجتماعي مثل الفيسبوك تصفحًا آمنًا عن طريق ضبط إعدادات الأمان للفيسبوك.

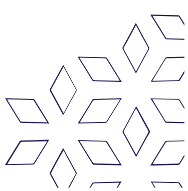


يُعرف التصفح الآمن بأنّه أحد الخدمات التي أطلَقها فريق الأمان الخاص بِشركة جوجل العالمية، وذلك بهدف تحديد مواقع الويب غير الآمنة عند تصفح الإنترنت وتنبيه المستخدمين وأصحاب تلك المواقع بالمخاطر المُتوقعة، ويَسمح التصفح الآمن بِاستعمال بنية تحتية خاصة تُتيح للمستخدم تَصفح المواقع الإلكترونية بِشكل محمي من أنواع مختلفة من الهجمات الإلكترونية كالبرامج الخبيثّة والضارة ومحاولات الاحتيال، وهُناك العديد من مُتصفحات الإنترنت التي تُستخدم لاستِعراض المواقع المختلفة، لِذا يجب اختيار متصفح الإنترنت الذي يتيح التصفح الآمن.

مميزات التصفح الآمن لشبكة الإنترنت

هُناك العديد من قواعد الاستخدام الآمن للإنترنت التي يجب الالتزام بها، إذ يُتيح التصفح الآمن عددًا من المزايا للمستخدمين، **وفيما يأتي توضيح أبرز مميزات التصفح الآمن:**

- التحقق من مواقع الويب ومُقارنتها مع قوائم التصفح الآمن للمواقع الضارة بِناءً على الاستراتيجية المُطبقة في موقع جوجل وأنواع التهديدات المُحتملة.
- تَنبيه المُستخدم قبل النقر على الروابط المَوجودة في أي موقع ويب والتي قد تَنقلُه إلى صفحات مليئة بالفيروسات.
- مَنع المُستخدم من نَشر أي روابط لِصفحات مَعروفة بأنّها خطيرة على أي موقع ويب.
- حِماية جميع مُستخدمي الويب من التصيد والبرامج الضارة والخبيثة من خِلال إشعارِهم بِمحاولة زِيارة موقع خطير.
- إتاحة مِيزة التصفح الآمن مجاناً من قبل شركة جوجل للشركات الأخرى لاستخدامِها في مُتصفحاتِهم وعَدم اقتِصاره على مُستخدمي كروم فقط لِجعل الإنترنت أكثر أماناً.
- حَظر المواقع غير المُلائمة للأطفال، إذ يساعد التصفح الآمن لشبكة الإنترنت على حماية الأطفال من مخاطر الإنترنت.



❖ المخاطر التي تهدد المستخدم أثناء تصفح الإنترنت

التطبيقات الخبيثة

برنامج يحمل حمولة مدمرة، ويتكرر وينتشر بسرعة لإصابة الأنظمة الأخرى. حيث إنه إلى حد بعيد، لا تزال الفيروسات / البرامج الضارة هي التهديد الأكثر انتشاراً للحوسبة.

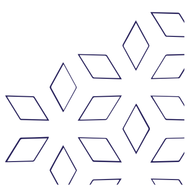
رسائل البريد المجهولة

يعتبر البريد الالكتروني وملحقات الرسائل الاكترونية الخطر الأكبر والسبب الرئيسي لانتقال أكثر من ٩٥% الفيروسات وهناك ملفات معينة تقوم بمهمة تقل الفيروسات ونشرها في أجهزة المستخدمين مثل الصور وملفات word و pdf وينصح عند تلقي رسالة من بريد الكتروني مجهول لك بعدم الرد عليها والأهم عدم فتح الملفات المرفقة معها.

التحميل من مواقع غيرموثوقة

يُنفّذ هذا الخطر من خلال استهداف مواقع الويب الضعيفة، وتحميل عدد من الرموز الخطيرة عليها، وفي حال دخول أحد المستخدمين لهذه المواقع سرعان ما يتعرّض النظام الخاص به للسرقة، أو التسبب بتعطل الخدمات الرئيسية فيه.

يُمكن الوقاية من خطر الهجوم من خلال تطبيق أمر إيقاف تشغيل البرامج النصية للصفحات، أو تثبيت الوظائف الخاصة بحظر البرامج النصية على المتصفح.



❖ خطوات التصفح الأمن من خلال الإنترنت

يُمكن تفعيل تصفح جوجل الآمن لِمتصفحات كروم في أجهزة الحاسوب باتِباع الخُطوات الآتية أدناه:

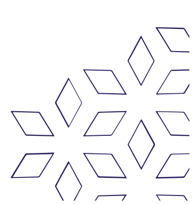
- فتح متصفح كروم على جهاز الحاسوب.
- الانتقال إلى أعلى يمين الشّاشة والضغط على الثلاث نقاط الرأسية، ثم اختيار الإعدادات (Settings).
- الانتقال إلى جزء الخصوصيّة والأمان (Privacy and security) ، والضغط على الأمان
- (Security) تحديد مستوى التصفح الآمن الذي يَرغب به المستخدم، **إذ تَظهر عدة خيارات وهي:** الحماية العادية، أو الحماية المحسنة، أو بلا حماية.

❖ السياسيات الأمنية في المؤسسات الصحية

تعرّف منظمة الصحة العالمية الصحة الإلكترونية بأنها الاستخدام الفعّال من حيث التكلفة والآمن لتكنولوجيات المعلومات والاتصالات في دعم المجالات المتصلة بالصحة، بما في ذلك خدمات الرعاية الصحية، والمراقبة الصحية، والمؤلفات الصحية، والتعليم الصحي، والمعرفة والبحوث الصحية.

هناك دليل واضح على التأثير المتنامي للصحة الإلكترونية على تقديم الرعاية الصحية في جميع أنحاء العالم حالياً، وكيف أنها تجعل النظم الصحية أكثر كفاءة وأكثر استجابة لاحتياجات الناس وتوقعاتهم.

ويشمل إقليم شرق المتوسط مستويات مختلفة من النضج والاستعداد للاستفادة من الصحة الإلكترونية باعتبارها محفزاً رئيسياً على تقديم خدمات الرعاية الصحية، وتدل التجربة على أن تسخير تكنولوجيا المعلومات والاتصالات من أجل الصحة يتطلب عمل استراتيجية متكاملة على المستوى الوطني، لتحقيق أفضل استخدام للقدرات القائمة في نفس الوقت الذي توفر فيه أساساً متينا للاستثمار والابتكار.



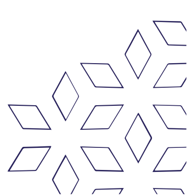
يُعدّ موفرو الرعاية الصحية من بين المؤسسات التي أكثر ما نثق بها، فهي بنى تحتية أساسية مهمة جداً لصحة العامة وسلامتهم، وفي حين أن المستشفيات تثق بالمعاهد الطبية، وتتعامل مختبرات الأبحاث مع الأصول الفريدة والقيّمة، تطورت تدفقات عمل جديدة ومهمة في هذا القطاع أدت إلى خلق تحديات أمنية جديدة ومسرّعة.

أصبحت الأنظمة الآن مترابطة ويتم استخدام الأجهزة المحمولة بشكل كبير لكل من الوصول عن بُعد ومشاركة البيانات، وتعرّض هذه الرقمنة بشكل متزايد مؤسسات الرعاية الصحية للهجمات العامة والمستهدفة.

كما دفع كوفيد ١٩ بالقطاع الصحي إلى صدارة أولويات الأمن الإلكتروني خلال عام ٢٠٢٠، إذ تمثل تهديدات الدول والمجرمين للأنظمة الصحية مصدر خطر متنامٍ.

ويواجه التحدي اللوجيستي الهائل الخاص بطرح اللقاحات خطر تعطيل السلاسل المعقدة للإمدادات.

كما تشكل برامج الفدية الإجرامية (برامج فيروسية تعطل الأنظمة الإلكترونية وتمنع مستخدميها من الوصول إلى بيانتهم، ويطالب مصنعوها بفدية مقابل إبطال عملها) تهديداً في وقت زاد فيه الوباء من اعتمادنا على التكنولوجيا.



❖ الأمان في مواقع التواصل الاجتماعي

التواصل مع أشخاص جدد هو شيء جيد ويمكن لمواقع التواصل الاجتماعية مثل فيسبوك وإنستغرام أن تساعدك على الشعور بالتواصل أكثر مع بلدك ان كنت مغتربا أو مع عائلتك، لكن مواقع التواصل الاجتماعية ممكن أن تكون خطرة، من المهم أن تفهم المخاطر حتى تتمكن من حماية نفسك.

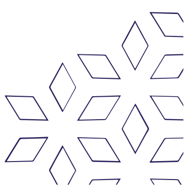
- **طرق حماية نفسك في وسائل التواصل الاجتماعي:**

- حماية بياناتك على مواقع التواصل الاجتماعي

تسمى معلوماتك الشخصية أحياناً بالبيانات، لا تحتاج أبداً إلى إعطاء بيانات شخصية مهمة، مثل أرقام الهوية، أو أرقام البنوك ،أو كلمات المرور أو عنوانك على مواقع التواصل الاجتماعي، للحفاظ على أمان مستخدميها، تحتوي الشبكات الاجتماعية على إعدادات خصوصية يمكنك استخدامه لجعل معلوماتك (البيانات) آمنة.

- حافظ على بياناتك آمنة على فيسبوك

عند وضع بياناتك على فيسبوك، وعند تسجيل الدخول إلى التطبيقات والمواقع، فإنك تتيح الوصول إلى بياناتك، قد تستخدم هذه التطبيقات و المواقع البيانات بطرق لا تريدها، في الغالب يستخدموها للسماح للمعلنين ببيع المنتجات لك، يمكنك إيقاف التطبيقات و المواقع من استخدام بياناتك، في فيسبوك، انتقل إلى إعداداتك، للعثور على الإعدادات، انقر فوق "**v**" (الرمز السفلي) في الزاوية اليمنى العليا من الشاشة وحدد "settings" ثم انقر على "Apps and Websites" في القائمة على اليسار، ثم سترى التطبيقات التي لديها حق الوصول إلى البيانات الخاصة بك، يمكنك النقر على كل تطبيق لـ تعديل ما يمكنهم الوصول إليه، للبقاء آمناً على وسائل التواصل الاجتماعي، يمكنك أيضاً حذف التطبيقات تماماً.



- **استخدام كلمات مرور قوية**

ينصحنا خبراء أمن الإنترنت دائماً بأن يكون لدينا كلمات مرور قوية ومختلفة لجميع حساباتنا، كما ينصحوننا بأستخدام المصادقة الثنائية (خطوات إضافية لتسجيل الدخول) أو أدارة كلمات المرور .

- **الحفاظ على الخصوصية على مواقع التواصل الاجتماعي**

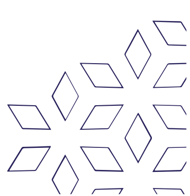
لا تشارك التفاصيل الشخصية أو الصور عبر الإنترنت التي تمانع في رؤيتها من أي شخص، مثل رئيسك في العمل، قد تعتقد أنك تشاركها فقط مع أصدقائك المقربين وعائلتك، ولكن بمجرد أن يكون هناك شيء عبر الإنترنت ، يمكن مشاركته على نطاق أوسع أيضاً ، بمجرد أن يكون على الانترنت ، لا يمكنك التخلص منه لأن الآخرين لديهم نسخ منه، تم طرد العديد من الأشخاص أو رفضوا للحصول على وظيفة بسبب ملفاتهم الشخصية على الإنترنت.

- **لا تصدق كل شيء ولا تصدق الجميع**

نحن نتعلم المزيد كل يوم حول كيف يتم استخدام وسائل التواصل الاجتماعي لخداع الناس، الكثير من المعلومات على وسائل التواصل الاجتماعي كاذبة، في بعض الأحيان، الناس على وسائل التواصل الاجتماعي ليسوا حتى أشخاصاً حقيقيين، وفي كثير من الأحيان لا تكون الأمور حقائق على الإطلاق، قد يكون هؤلاء الأشخاص مع أسماء كاذبة أو bot (a fake robot) قد تكون تقارير إخبارية مزيفة أو رسائل رسمية تتظاهر بأنها من مسؤول حكومي أو مسؤول تجاري.

–لا تصدق كل ما تقرأه على وسائل التواصل الاجتماعي إذا كنت تقرأ شيئاً ما، فتحقق من مصادر أخرى، مثل الموقع الإلكتروني لصحيفة وطنية.

–إذا تلقيت رسالة عبر الإنترنت تقول إنها من الحكومة أو شركة، فلا ترد بمعلوماتك الشخصية.



- **البقاء آمناً دون اتصال، أيضاً**

فكر في أمانك في العالم الحقيقي عند نشر معلومات حول أنشطتك، لا تحتاج إلى نشر عنوانك عبر الإنترنت ثم نشر صور العطلة لإعلام الجميع بأنك بعيد، إذا كنت تنشر على الفيسبوك قضاء العطلة خارجاً مع عائلتك، سيعرف الناس أن منزلك فارغ.

بالإضافة إلى ذلك، قد تقوم أحياناً بنشر مكان تواجدك أو الدخول "check into" إلى الأماكن، فكر إذا كان يجب عليك القيام بذلك أم لا.

- **كن حذر جداً إذا كنت تلتقي بشخصٍ ما**

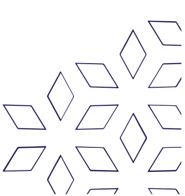
تسهل وسائل التواصل الاجتماعي على الناس تعويض الهويات، على الانترنت، يمكنهم التظاهر بأنهم شخص آخر، إذا كنت تتصل مع شخص ما عبر الإنترنت، لا ترتب أبداً لمقابلة هذا الشخص بمفرده أو الذهاب إلى منزله أو دعوته إلى منزلك إلا إذا كنت تعرف بأنهم من يدعون فعلاً، أجتمع بالغرباء دائماً في مكان عام وعندما يكون هناك أشخاص آخرين حولكم.

- **عدم إرسال الأموال أو كلمات المرور**

لا ترسل الأموال إلى أي شخص عندما لا تكون متأكداً ١٠٠٪ منهم، المكاتب الحكومية، مثل IRS ، والشركات الحقيقية، مثل مايكروسوفت، لا تطلب منك إرسال الأموال مباشرة إلى حسابات مصرفية غريبة، كما أنهم لا يطلبون كلمة المرور الخاصة بك إلى أي شيء، لا ترسل كلمة المرور الخاصة بك إلى أي شخص تلتقي به من مواقع التواصل الاجتماعية أو أماكن أخرى على الإنترنت.

- **حماية نفسك من الأشخاص العدائيون أو غير اللطفاء**

يستهدف الناس المعادون أو غير اللطفاء اللاجئين والمهاجرين، لا تقبل طلبات الصداقة من أشخاص لا تعرفهم، قم على الفور بحظر أي شخص ينشر شيئ مهدد على أي من حساباتك لاترد, لا تكتب أشياء فظة أو عدائية قد تجعلك أكثر من هدف، قم بالإبلاغ عن التهديدات الشخصية للشرطة وموقع التواصل الاجتماعي الذي تم نشره عليه.



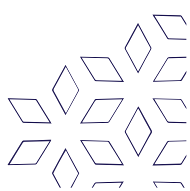
- حماية نفسك من الحيل والمخترقون

لا تنقر على الروابط فقط لأنها ترسل إليك، حتى لو كانت تأتي من صديق (قد لا يعرفون أن الرابط خطير، أو ربما تم اختراقه) فقط قم بحذفها، لن يتم إرسال أي شيء مهم لك بهذه الطريقة، من المرجح أن تحتوي الروابط التي لم تطلبها على فيروسات من شأنها أن تضر جهازك أو تسمح للأشخاص بالدخول إلى جهازك لسرقة معلوماتك وأموالك وهويتك، وتذكر **any offer that seems too good to be** : **true IS too good to be true!** **إذا أستلمت رسالة تقول أنك ستحصل على الكثير من المال من شخص لا تعرفه، فأحذفها.**

- حافظ على سلامة أطفالك

حتى إذا كنت لا تستخدم وسائل التواصل الاجتماعية أو تفهمها، فستحتاج إلى معرفة ما يكفي حول هذا الموضوع للحفاظ على أطفالك في مأمن من مخاطر مواقع التواصل الاجتماعي، إذا كنت تستخدم وسائل التواصل الاجتماعية بنفسك، أحمي أطفالك بعدم وضع معلومات عنهم عبر الإنترنت، إذا كنت لا تستخدم وسائل التواصل الاجتماعية، اسأل أطفالك عن الشبكات الاجتماعية التي يستخدموها، يمكن أن يتعرضوا للتنمر، وللمفترسين الجنسيين، وللمحتوى السيئ، والإعلان.

يوصي العديد من خبراء التكنولوجيا فقط السماح للأطفال الصغار بأستخدام الهاتف الذكي أو الكمبيوتر أمامك، سيكون عليك أن تقرر لطفلك، ولكن معظم الخبراء ينصحون بعدم السماح للأطفال بالحصول على هواتف ذكية أو أجهزة كمبيوتر في غرفهم ليلاً.



❖ حماية البيانات الشخصية في التجارة الالكترونية

التجارة الالكترونية تعني ممارسة الاعمال التجارية على شبكة الانترنت وتشمل عمليات بيع وشراء السلع او الخدمات عبر الانترنت، في الوقت الحاضر العديد من الشركات ذات السمعة الطيبة مقبلة على هذا النمط من ممارسة الاعمال التجارية لتغطية سوق أوسع، ويغطي الامن الالكتروني او امن الانترنت مجموعة واسعة من الانشطة للحفاظ على المعلومات الالكترونية الامنة، وتجري عمليات الشراء والاعمال التجارية عبر الانترنت اكثر واكثر كل يوم لذلك من المهم بالنسبة للمستخدمين فهم كيفية حماية البيانات الشخصية على اجهزة حواسيبهم وخلال معاملاتهم المالية اذا ارادوا المشاركة في التجارة الالكترونية وشراء احتياجاتهم عبر الانترنت.

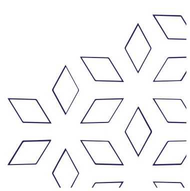
البيانات الشخصية

البيانات الشخصية هي البيانات الهامة لكل شخص والتي يتم تداولها عادة عند اجراء عمليات متعلقة بالتجارة الالكترونية، **ومنها ما يلي:**

- الاسم والعنوان
- ارقام الهاتف
- البريد الالكتروني
- كلمة السر للحسابات
- البيانات المالية
- البيانات الاجتماعية

المقصود بحماية البيانات الشخصية

حماية البيانات الشخصية تعني حماية المعلومات المتعلقة بشخص الفرد وحياته الخاصة من التعرض للاعتداء وخاصة في ظل التحديات الرقمية.



اجراءات الامان عند التعاملات الالكترونية

توجد عدد من الاجراءات التي يمكن اتباعها لتحقيق الامان عند التعاملات الالكترونية **ومنها ما يلي:**

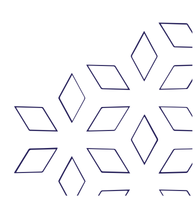
- استخدام بروتوولات الامان العالمية المتعددة
- استخدام وسائل الدفع الامنة
- عدم مشاركة البيانات الشخصية
- اختيار كلمة مرور قوية
- عدم التصريح لاي شخص بكلمة السر
- الحفاظ على المعلومات البنكية
- التأكد من المواقع التي يتم التعامل من خلالها

❖ التحقق الرقمي من الهوية

الهوية الرقمية هي وسيلة إلكترونية لتعريف الشخص، وتتكون من شهادة تحتوي على مفتاح عام يمكن مشاهدته ومفتاح خاص يظل سراً.

يتيح لك المفتاح الخاص التوقيع على مستند إلكتروني بتوقيع يمكن للآخرين التحقق منه باستخدام المفتاح العام الخاص بك فقط. وبالمثل، يمكن للمفتاح الخاص إلغاء تشفير المستندات التي قام آخرون بتشفيرها باستخدام المفتاح العام الخاص بك.

لقبول الهوية الرقمية كعنصر صالح، يجب أن يثق المستلم بها، للمساعدة في ضمان أصالة الهوية الرقمية، توفر جهات إصدار الشهادات هويات رقمية للأشخاص الذين تم التحقق من هوياتهم.

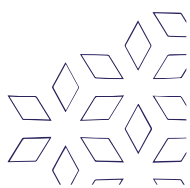


التحقق من الهوية الرقمية

خلال العقد الماضي ارتفعت توقعات المستخدمين من القدرات الرقمية بشكل كبير، فما كنا نحسبه كماليات أصبح بمنظور عصرنا الحالي أساسيات، ولا يمكن قبوله بأي حال من الأحول على أنه رفاهية إضافية؛ فالكل في يومنا هذا يسعى للحصول على إجراءات مبسطة بغض النظر عن الجهة التي يتعاملون معها أو طبيعة الأداة الرقمية المتاحة لهذا التعامل.

الإجراءات المبسطة أو السهلة تكون دائما بإزالة جميع العقبات من كل مرحلة من مراحل دورة حياة الإجراء، وهذا بدوره يتطلب تكاملا رقميا مباشرا بين جميع قنوات الخدمة المتاحة فيما بينها وكذلك مع جميع الأنظمة التي تعمل خلف ذلك(Back Office Solutions) ، هذا التكامل وهذه السهولة خلقت تحدياً أمنياً في الصناعات الرقمية فيما يتعلق بالحفاظ على خصوصية البيانات، وربما يظهر ذلك جليا بشكل واضح في التعاملات المصرفية، فأنت من خلال تطبيق جوالك قادر على إدارة كافة تعاملاتك المصرفية بكل سهولة وفي نفس الوقت على المصرف اتخاذ كافة الإجراءات اللازمة لضمان أن من يقوم بهذه الإجراءات هو الشخص المعني.

في الماضي كان ذلك سهلاً من خلال تواجدك في الفرع وإتمامك جميع الإجراءات بشكل شخصي، حيث يستطيع موظف البنك التحقق من هويتك بكل سهولة، لذا، في هذا العالم الرقمي، كيف يمكنك إنشاء إجراءات صارمة للتحقق من الهوية والتي تكون أيضاً سهلة من وجهة نظر العميل؟

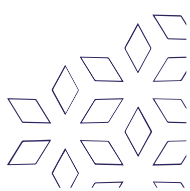


قبل الانتقال للإجابة على هذا التساؤل، يجب توضيح الآتي، الهوية الرقمية المقصودة في حوارنا هذا هي المعرّفات التي تحتاجها الجهة للتأكد من أن مستخدم النظام هو الشخص المعني بذلك وليس شخص آخر، وهذا المفهوم يختلف اختلافا كليا عن النسخة الرقمية من الهوية الشخصية التي باتت تستخدم بكثرة في كافة الدول المتقدمة، مثل الهوية الرقمية المرتبطة بتطبيق أبشر في المملكة العربية السعودية، فهذه الهوية هي نسخة إلكترونية فقط حلت مكان الهوية الشخصية المتعارف عليها، وهي لا تغني عن إجراءات التحقق اللازمة التي يقدمها تطبيق أبشر لتوثيق بيانات المستخدم والتحقق منه.

عودة لسؤالنا عن أهم الإجراءات اللازمة لتتحقق من الهوية مع الحفاظ على السهولة والتجربة الرائعة للمستخدم، بكل بساطة يمكننا القول إنها تبدأ ضمن عملية تطوير كافة إجراءات خدمة العملاء من البداية(Customer Onboarding Journey) ، وبذلك يظهر لنا تساؤل جديد، ما هي رحلة انضمام العميل؟ ولماذا نحتاج إلى تطويرها؟

تعرف رحلة انضمام العميل بأنها مجموعة الإجراءات التي يتخذها المستخدم للبدء باستخدام منتج أو خدمة معينة للمؤسسة، بحيث تشكل هذه الإجراءات الانطباع الأولي للمستخدم عن المؤسسة وما تقدمه من خدمة، **وعادة ما تتضمن هذه الرحلة الخطوات التالية:**

- جمع المعلومات الشخصية للمستخدم
- التحقق من هوية المستخدم
- تحديد خيرات الخدمة أو المنتج المطلوبة
- تعريف بيانات الدفع
- تأكيد إتمام عملية تجميع المعلومات



تاسعاً: وسائل الأمن المادي وأساليب أمن التقنيات المختلفة

في هذا الفصل سنتعرف على المواضيع التالية:

- مفهوم الأمن المادي وخصائصه
- أهمية الأمن المادي
- أنظمة الأمن المادي
- الحماية المادية لمركز البيانات
- أمن البيانات الضخمة
- أمن الهواتف النقالة
- المواطنة الرقمية
- الأمن الرقمي
- الاتصالات الرقمية

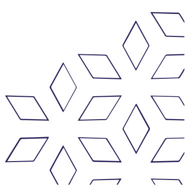
❖ مفهوم الأمن المادي وخصائصه

يصف الأمن المادي Physical security التدابير الأمنية security التي تم تصميمها لمنع الوصول غير المصرح به إلى المرافق والمعدات والموارد، وحماية الأفراد والممتلكات من التلف أو الضرر (مثل التجسس Espionage أو السرقة Theft، أو الهجمات الإرهابية Terrorist) ينطوي الأمن المادي على استخدام طبقات متعددة من نظم مترابطة، تشمل الدوائر التلفزيونية المغلقة CCTV، وحراس الأمن Security guards، حواجز واقية Protective barriers، والأقفال locks، وبروتوكولات التحكم في الوصول Access control ، والعديد من التقنيات الأخرى.

❖ أهمية الأمن المادي

تهدف أنظمة الأمن المادي للمرافق المحمية عموماً إلى:

- ردع المتسللين المحتملين (مثل علامات التحذير وعلامات الحدود الخارجية).
- تمييز الأشخاص المأذون لهم من غير المصرح لهم (مثل استخدام بطاقات المفاتيح / شارات الوصول).
- تأخير، إحباط، ومنع محاولات التسلل (مثل الجدران قوية، وأقفال الأبواب وخزائن).
- كشف الاختراقات ورصد / تسجيل الدخلاء (مثل أجهزة الإنذار عن الدخلاء وأنظمة الدوائر التلفزيونية المغلقة)
- إطلاق ردود الفعل المناسبة (على سبيل المثال من قبل حراس الأمن والشرطة)



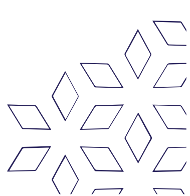
❖ أنظمة الأمن المادي

طرق الردع

هدف الردع هي إقناع المهاجمين المحتملين بأن الهجوم الناجح غير مرجح بسبب الدفاعات القوي، طبقة الأمان الأولية للحرم الجامعي، أو المبنى، أو المكتب أو استخدامات المساحة المادية الأخرى منع الجريمة من خلال التصميم البيئي لردع التهديدات، بعض الأمثلة الأكثر شيوعاً هي أيضاً الأكثر أساسية: علامات التحذير أو ملصقات النوافذ، الأسوار، حواجز المركبات، قيود ارتفاع السيارة، نقاط الوصول المقيدة، الإضاءة الأمنية والخنادق.

حواجز طبيعية

تعمل المسامير فوق الجدار الفاصل كرادع للأشخاص الذين يحاولون التسلق فوق الجدار، تعمل الحواجز المادية مثل الأسوار والجدران وحواجز المركبات كطبقة خارجية من الأمان، إنها تعمل على منع ، أو على الأقل تأخير ، الهجمات ، وتعمل أيضاً كرادع نفسي من خلال تحديد محيط المنشأة وجعل عمليات الاقتحام تبدو أكثر صعوبة، غالباً ما يتم وضع سياج طويل يعلوه أسلاك شائكة أو أسلاك شائكة أو مسامير معدنية على محيط العقار ، مع نوع من اللافتات التي تحذر الأشخاص من محاولة الدخول، ومع ذلك ، في بعض المرافق ، لن يكون من الممكن فرض جدران / سياج محيطي (على سبيل المثال ، مبنى مكاتب حضري مجاور مباشرة للأرصفة العامة) أو قد يكون غير مقبول من الناحية الجمالية (على سبيل المثال ، إحاطة مركز تسوق بأسوار طويلة تعلوها أسلاك شائكة) ؛ في هذه الحالة ، سيتم تعريف محيط الأمان الخارجي على أنه جدران / نوافذ / أبواب الهيكل نفسه.

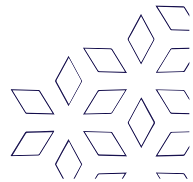


حواجز الجمع

درع فولاذي، عرض تشوه البلاستيك نتيجة ل قذيفة التأثيرات، يمكن أن يتسبب تشوه اللدائن الناتج عن الاصطدام في حدوث خلخلة أو تمزق أو سحق الحماية السلبية من الحرائق(PFP) ، لا سيما بمجرد التأكيد على مواد PFP يمكن أن تكون بعض مواد PFP أحياناً شديدة المرونة ومقاومة للصدمات وقابلة للدكت في المحيط، بمجرد الإجهاد بالنار، يمكن أن يتغير ذلك مع تبدد الماء الحر عند ١٠٠ درجة مئوية (٢١٢ درجة فهرنهايت)، ويمكن إنفاق الهيدرات بالقرب من ٣٠٠ درجة مئوية (٥٧٢ درجة فهرنهايت)، والتي يتم الوصول إليها جميعاً في غضون دقائق من الحريق، يمكن أن تتحلل روابط مستوى البناء، على عكس بعض الحراريات، أيضاً مع الحرارة، وبالتالي تغيير الخصائص الفيزيائية للعديد من مواد PFP عبر نطاقات درجات حرارة مختلفة، لا شيء من ذلك عادة يمثل مشكلة، في الواقع هو جزء من تصميمات PFP لأسباب مختلفة، ولكن عند الجمع بين PFP مع المقذوفات أو التجزئة، من الحكمة مراعاة جميع الضغوط ذات الصلة في تصميم الحواجز التي يجب (أو يمكن افتراضها أو الإعلان عنها) في نفس الوقت هزيمة الحريق، متبوعاً بتيار خرطوم والتأثيرات التي تحدث أثناء حريق.

تم تصميم الحواجز عادة لهزيمة التهديدات المحددة، هذا جزء من ارقام المباني وكذلك رموز الحريق، بصرف النظر عن التهديدات الخارجية، هناك تهديدات داخلية نار وهجرة الدخان وكذلك التخريب.

يشير قانون البناء الوطني لكندا، على سبيل المثال، إلى الحاجة إلى هزيمة الانفجارات الخارجية باستخدام مغلف المبنى حيث تكون ممكنة، مثل الأماكن الكهربائية الكبيرة ،محولات تقع بالقرب من مبنى حواجز الحريق ، محولات الجهد العالي يمكن أن تكون أمثلة على الجدران المصممة لهزيمة الحرائق والمقذوفات والتفتت في وقت واحد نتيجة لتمزق المحولات، وكذلك نيران الأسلحة الصغيرة الواردة، وبالمثل، قد تحتوي المباني على حواجز داخلية لتدمير الأسلحة وكذلك النار والحرارة، مثال على ذلك هو عداد في مركز شرطة أو سفارة، حيث يمكن للجمهور الوصول إلى غرفة، ولكن التحدث من خلال الزجاج الأمني للموظفين في الخلف، إذا كان هذا الحاجز يتماشى مع حجرة الحريق كجزء من الامتثال لقانون البناء، فيجب هزيمة التهديدات المتعددة في وقت واحد، والتي يجب أخذها في الاعتبار في التصميم.

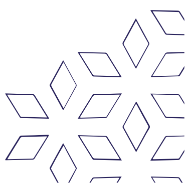


المراقبة الطبيعية

شكل رئيسي آخر من أشكال الردع التي يمكن دمجها في تصميم المرافق هو المراقبة الطبيعية، حيث يسعى المهندسون المعماريون إلى بناء مساحات أكثر انفتاحاً ومرئية لموظفي الأمن والمستخدمين المصرح لهم، بحيث لا يتمكن المتسللون / المهاجمون من أداء نشاط غير مصرح به دون رؤيتهم، مثال على ذلك هو تقليل كمية النباتات الطويلة الكثيفة في المناظر الطبيعية حتى لا يتمكن المهاجمون من إخفاء أنفسهم بداخله، أو وضع موارد مهمة في مناطق حيث يتعين على المتسللين عبور مساحة واسعة ومفتوحة للوصول إليهم (مما يجعل من المحتمل أن يلاحظهم شخص ما).

الإضاءة الأمنية

الإضاءة الأمنية هو شكل آخر فعال من أشكال الردع. يقل احتمال دخول المتسللين إلى مناطق جيدة الإضاءة خوفًا من رؤيتهم. يجب أن تكون الأبواب والبوابات والمداخل الأخرى، على وجه الخصوص، مضاءة جيدًا للسماح بالمراقبة الدقيقة للأشخاص الذين يدخلون ويخرجون. عند إضاءة أرض المنشأة، تكون الإضاءة المنخفضة الكثافة الموزعة على نطاق واسع أفضل بشكل عام من البقع الصغيرة للإضاءة عالية الكثافة، لأن الأخيرة قد تميل إلى إنشاء نقاط عمياء لأفراد الأمن وكاميرات الدوائر التلفزيونية المغلقة، من المهم وضع الإضاءة بطريقة تجعل من الصعب العبث بها (مثل تعليق الأضواء من الأعمدة العالية)، والتأكد من وجود مصدر طاقة احتياطي حتى لا تنطفئ أضواء الأمان إذا انقطع التيار الكهربائي، أتاح إدخال منتجات الإضاءة القائمة على LED منخفضة الجهد إمكانات أمنية جديدة، مثل التشغيل الفوري أو القوية ، مع تقليل استهلاك الكهرباء بشكل كبير.

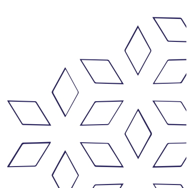


كشف التسلل والمراقبة الإلكترونية

- **أنظمة الإنذار وأجهزة الاستشعار**

أنظمة الإنذار يمكن تثبيتها لتنبيه أفراد الأمن عند محاولة الوصول غير المصرح به، تعمل أنظمة الإنذار جنبًا إلى جنب مع الحواجز المادية والأنظمة الميكانيكية وحراس الأمن، مما يؤدي إلى إطلاق استجابة عندما يتم اختراق هذه الأشكال الأخرى من الأمان، وهي تتكون من أجهزة استشعار بما في ذلك مجسات المحيط، مجسات الحركة ومستشعرات الاتصال وكاشفات كسر الزجاج

ومع ذلك، تكون الإنذارات مفيدة فقط إذا كانت هناك استجابة سريعة عند إطلاقها، في مرحلة الاستطلاع السابقة للهجوم الفعلي، سيختبر بعض المتسللين وقت استجابة أفراد الأمن لنظام إنذار متعثّر بشكل متعمد، من خلال قياس المدة التي يستغرقها فريق الأمن للوصول (إذا وصلوا على الإطلاق) ، يمكن للمهاجم تحديد ما إذا كان الهجوم يمكن أن ينجح قبل وصول السلطات لتحييد التهديد، يمكن أيضاً أن تعمل الإنذارات الصوتية العالية كرادع نفسي، من خلال إخطار المتسللين بأنه تم اكتشاف وجودهم ، في بعض الولايات القضائية ، لن تستجيب جهات إنفاذ القانون للإنذارات الصادرة عن أنظمة الكشف عن التسلل ما لم يتم التحقق من التنشيط بواسطة شاهد عيان أو مقطع فيديو، تم وضع سياسات مثل هذه لمكافحة معدل ٩٤–٩٩ بالمائة لتنشيط الإنذار الكاذب في الولايات المتحدة.



- **المراقبة بالفيديو**

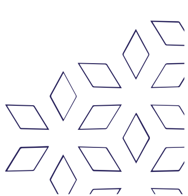
كاميرات الدوائر التلفزيونية المغلقة

كاميرات المراقبة يمكن أن يكون رادعا عند وضعها في مواقع مرئية للغاية وتكون مفيدة لتقييم الحوادث والتحليل التاريخي، على سبيل المثال، إذا تم إنشاء إنذارات وكانت هناك كاميرا في مكانها، يقوم أفراد الأمن بتقييم الموقف عبر موجز الكاميرا، في الحالات التي حدث فيها هجوم بالفعل وكانت الكاميرا في مكانها عند نقطة الهجوم، يمكن مراجعة الفيديو المسجل، على الرغم من أن المصطلح الدوائر التلفزيونية المغلقة (CCTV) شائعة، وسرعان ما أصبحت قديمة لأن المزيد من أنظمة الفيديو تفقد الدائرة المغلقة لنقل الإشارات وبدلاً من ذلك يتم الإرسال على كاميرا IP الشبكات.

لا تضمن مراقبة الفيديو بالضرورة استجابة بشرية، يجب أن يقوم الإنسان بمراقبة الوضع في الوقت الفعلي من أجل الاستجابة في الوقت المناسب، خلاف ذلك، فإن مراقبة الفيديو هي مجرد وسيلة لجمع الأدلة لتحليلها لاحقاً، ومع ذلك، التقدم التكنولوجي مثل تحليلات الفيديو تقلل من حجم العمل المطلوب لمراقبة الفيديو حيث يمكن إخطار أفراد الأمن تلقائياً بالأحداث الأمنية المحتملة.

- **صلاحية التحكم صلاحية الدخول**

صلاحية التحكم صلاحية الدخول يتم استخدام الطرق لمراقبة حركة المرور والتحكم فيها من خلال نقاط وصول ومناطق محددة في المنشأة الآمنة، يتم ذلك باستخدام مجموعة متنوعة من الأنظمة بما في ذلك CCTV مراقبة، بطاقات هوية، حراس الأمن، القراء البيومترية وأنظمة التحكم الإلكترونية / الميكانيكية مثل الأقفال، والأبواب والأبواب الدوارة والبوابات.



- **أنظمة التحكم في الوصول الميكانيكية**

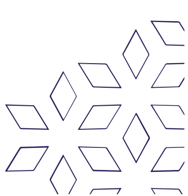
الباب الدوار البصري ذو الذراع المسقطة، نظام إلكتروني للتحكم في الدخول، يتحكم في الدخول من خلال باب.

أنظمة التحكم في الوصول الميكانيكية تشمل الأبواب الدوارة، والبوابات والأبواب والأقفال، مفتاح التحكم من الأقفال مشكلة مع عدد كبير من المستخدمين وأي معدل دوران للمستخدمين، مفاتيح سرعان ما يصبح غير قابل للإدارة، مما يؤدي في كثير من الأحيان إلى اعتماد التحكم الإلكتروني في الوصول.

- **أنظمة التحكم في الدخول الإلكترونية**

التحكم الإلكتروني في الوصول يدير عدداً كبيراً من المستخدمين ، ويتحكم في أوقات دورات حياة المستخدم والتواريخ ونقاط الوصول الفردية، على سبيل المثال ، يمكن أن تسمح حقوق الوصول للمستخدم بالوصول من الساعة ٠٧٠٠ إلى الساعة ١٩٠٠ من الاثنين إلى الجمعة وتنتهي الصلاحية في غضون ٩٠ يوماً [بحاجة لمصدر] غالباً ما يتم ربط أنظمة التحكم في الوصول هذه بأبواب دوارة للتحكم في الدخول في المباني لمنع الوصول غير المصرح به، يقلل استخدام البوابات الدوارة أيضاً من الحاجة إلى أفراد أمن إضافيين لمراقبة كل فرد يدخل المبنى مما يسمح بإنتاجية أسرع.

يتم الوصول إلى طبقة فرعية إضافية من الحماية الميكانيكية / الإلكترونية للتحكم في الوصول من خلال دمج a ادارة المفاتيح نظام لإدارة حيازة واستخدام المفاتيح الميكانيكية للأقفال أو الممتلكات داخل المبنى أو الحرم الجامعي.

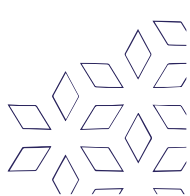


- **نظم تحديد الهوية وسياسات الوصول**

شكل آخر من أشكال التحكم في الوصول (إجرائية) يشمل استخدام السياسات والعمليات والإجراءات لإدارة الدخول إلى المنطقة المحظورة، مثال على ذلك هو نشر أفراد الأمن الذين يقومون بفحص الدخول المصرح به في نقاط الدخول المحددة مسبقاً، عادة ما يتم استكمال هذا الشكل من أشكال التحكم في الوصول بالأشكال السابقة للتحكم في الوصول (أي التحكم في الوصول الميكانيكي والإلكتروني)، أو الأجهزة البسيطة مثل الممرات المادية.

- **أفراد الأمن**

أفراد الأمن تلعب دوراً مركزياً في جميع مستويات الأمان، جميع الأنظمة التكنولوجية المستخدمة لتعزيز الأمن المادي غير مجدية بدون قوة أمنية مدربة على استخدامها وصيانتها، والتي تعرف كيف تستجيب بشكل صحيح للانتهاكات الأمنية، يقوم أفراد الأمن بالعديد من الوظائف: تسهيلات الدوريات ، وإدارة التحكم في الوصول الإلكتروني ، والرد على الإنذارات ، ومراقبة وتحليل لقطات الفيديو.



❖ الحماية المادية لمركز البيانات

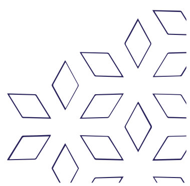
مركز البيانات، في أبسط صوره، عبارة عن مرفق مادي تستخدمه المؤسسات لإيواء تطبيقاتها وبياناتها المهمة، يستند تصميم مركز البيانات إلى شبكة من موارد الحوسبة والتخزين التي تمكّن تسليم بيانات وتطبيقات البرامج التي تمت مشاركتها، تشمل المكونات الرئيسية لتصميم مركز البيانات أجهزة التوجيه، والمبدلات، وجدران الحماية، وأنظمة التخزين والخوادم ووحدات التحكم في تسليم التطبيقات.

ليس من المفيد الحصول على جميع المعدات وأحدث أنظمة تكنولوجيا المعلومات في مركز البيانات التي ليس لديها رقابة صارمة على أنظمة الدخول والخروج.

يقول جوستافو ريزو، الرئيس التنفيذي لشركة فولت: "مع تطور التكنولوجيا والحلول السحابية، لم يتم اختبار أمن مراكز البيانات أبدا من قبل"

يجب أن يقال إنه في مراكز البيانات الكبيرة والتي توفر استضافة المواقع والبيانات، يمكن لمئات العملاء زيارة الخوادم الخاصة بك في أي لحظة، مما يجعل هناك مخاطر وصعوبات لضمان حماية المعلومات، ويقول ريزو " يكذب على نفسه من يظن أن هذه الهياكل والشركات هي ضحية للجرائم الظاهرية والغزوات على الانترنت"

لهذا، إلى جانب منع التهديدات المادية مثل النار والحرارة والدخان والغازات المسببة للتآكل والتسريبات والانفجارات، يجب الأخذ في الاعتبار خطر الدخول إلى مركز البيانات والوصول إلى الراكات والسيرفرات، وبعبارة أخرى، ينبغي أن يضمن الفحص الفعال للمستخدمين المسموح لهم، وفي الوقت نفسه، منع التطفل، والتغيير، والسرقة، والأضرار التي تلحق بالمعدات وكذلك سرقة البيانات.



ويقول أوزوالدو أوجيام، مدير جمعية الأمن الإلكتروني البرازيلية: "يقدم قطاع مراقبة الدخول والخروج اليوم عددا لا يحصى من التقنيات التي تسمح بتحديد ومراقبة وتتبع الأشخاص والأجهزة تلقائياً وهي تعمل بتكامل مع أنظمة الإنذار وأنظمة المراقبة بالكاميرات".

في العشر سنوات الأخيرة، استمر سوق الأنظمة الإلكترونية الأمنية في النمو بمعدل سنوي ١٠٪ وفي عام ٢٠١٣، ازداد هذا القطاع بنحو ١,٤٦ مليار دولار امريكي، منها ٢١% لأنظمة م في الدخول والخروج، فيما كان يتمثل الجزء الأكبر وهو ٤٦% لقطاع المراقبة بالكاميرات يليها أنظمة الإنذار بنسبة ٢٣%.

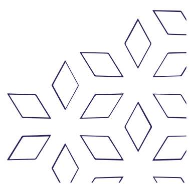
كما أن ضمان التحكم في الدخول والخروج في مراكز قواعد البيانات هو أيضا من الأمور الهامة جدا للشركات التي تقوم بعمل شهادات رقمية، كما أنشأها المعهد الوطني لتقنية المعلومات (البرازيل)، الذي ينشأ قواعد الشهادات الرقمية في البرازيل ويضمن صحة والصلاحية القانونية في الطرق الإلكترونية.

الطبقات

حماية مراكز البيانات تتبع مفهوم "الطبقات"، أي أنه يجب أن تبدأ الحماية من الطبقة الخارجية، والمنطقة المحيطة ثم الذهاب الى جميع الطبقات الداخلية: الطوابق، الغرف، الراكات والسيرفرات.

تستطيع أجهزة التحكم في الدخول والخروج الكشف وإعطاء ما يكفي من الوقت لاتخاذ التدابير المناسبة، مثال على حماية المناطق المحيطة بالمباني هي الحواجز، وحدات التحكم التي تسمح بمرور المركبات الثقيلة، ويتكون النظام من الحواجز الهيدروليكية الأتوماتيكية، وقال ريزو "ان المعدات تستخدم بالفعل على نطاق واسع في أوروبا، ومعظمها ضد هجمات إرهابية بسيارة مفخخة"

في مراكز البيانات، الركات المغلقة، غرف الخادم ووحدات المعالجة المركزية يكون التدبير الأول هو حماية الشبكة. ففي حالة ما إذا كانت الشركة صغيرة يمكن التحكم في ذلك عن طريق المفاتيح. ولكن ماذا عن مراكز البيانات التي تحتوي على الالاف من الراكات؟، كيف يمكن الإدارة والتحكم في عدد لا يحصى من عمليات الدخول والخروج وإجراء عمليات متابعة دقيقة؟ وكيف يمكن تخصيص أوقات الدخول والخروج تبعا للمنطقة والمستخدمين؟



ولتخطي هذه العقبة، طورت فولت وحدة تحكم تعمل مع برنامج والذي يسمح لقارئ واحد في ٣٢ باب وحساس وجعل الاستثمار ممكنا، ويقول ناتان كوجلوفيتشي، مدير قسم الهندسة في فولت: "إن مشروع به ٣٢٠ راك، يحتاج فقط إلى ١٠ وحدات تحكم و١٠ قوارئ، يتم توصيلها مع ٣٢٠ قفل وأجهزة استشعار"، ويكون الدخول عن طريق الكارت، بصمة او غيرها.

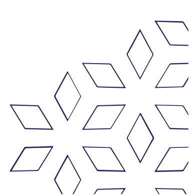
يمكن لأنظمة التحكم في الدخول والخروج العمل بطريقة متكاملة مع أنظمة إنذار الحريق إنذار السرقة من خلال وحدات التحكم SCAIIP ،

نظام فولت والذي يعمل من خلال TCP/IP Protocol ، يستطيع التحكم في دخول وخروج المشاة أو السيارات، رصد أجهزة الإنذار، جولة الحراس، التحكم في المصاعد، التحكم في الراكات، الكاميرات وغيرها من المميزات.

ففي مشروع الشهادات الرقمية، قامت فولت بتنفيذ نظام أمني متكامل (تحكم في الدخول والخروج/ كاميرات مراقبة / إنذار السرقة / إنذار الحريق) لحماية غرفة فولت في ساو باولو وريو دي جانيرو.

وفقاً لما يقول ريزو، لقد تم تصميم النظام بشكل محدد للتحكم والسيطرة على فتح ومراقبة أبواب الراك للسيرفرات.

"مراكز البيانات لديها عدد كبير جدا من الأبواب التي يمكن التحكم فيها والسيطرة عليها، تصل في كثير من الأحيان إلى مئات أو آلاف، ولأن نظام التحكم في الدخول والخروج التقليدي سيكون مكلفاً، وأيضا غير مجدي، ليس فقط من الناحية الاقتصادية، ولكن أيضا من قبل متطلبات البنية التحتية الكبيرة والمعقدة" .



وفقا لإدارة ممارسة التحكم في الدخول والخروج، فإنه يجب على أنظمة التحكم في الدخول والخروج أن تتبع الخطوات الاتية:

–تحديد الهوية: يتم التحقق من الهوية والتحقق من صحتها من خلال وثائق التفويض التي يمكن تقديمها خلال مرحلة تحديد الهوية.

–المصادقة: تحديد الحقوق والأذونات التي يمتلكها مستخدم النظام، بعد المصادقة، تحدد عملية التفويض ما إذا كان لديه حق الوصول إلى المكان أو لا.

–التدقيق: هو مرجع للمعلومات التي تم جمعها والمتعلقة بالاستخدام، من قبل المستخدمين للنظام، ويمكن استخدام هذه المعلومات للإدارة، والتخطيط، وما إلى ذلك.

يحدث التدقيق في الوقت نفسه عندما يتم تبادل المعلومات المتعلقة بالمستخدم في لحظة استخدام نظام إدارة التحكم في الدخول والخروج، يتم تسجيل بيانات التدقيق في الذاكرة ومن ثم إرسالها في وقت لاحق، عادة ما تكون المعلومات المتعلقة بهذه العملية هي هوية المستخدم، طبيعة الخدمة، البداية والنهاية.

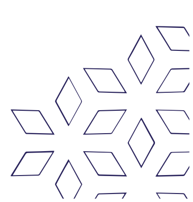
<u>البصمات</u>

تعتمد أنظمة فولت على تكنولوجيا قراءة البصمات من بصمات الأصابع والتعرف على الوجه.

مما يسمح للتطبيق في مختلف الظروف، أما بالنسبة للأقفال، والتي يمكن أن تستخدم أيضاً لزيادة أمن مركز البيانات، توجد نماذج محددة لكل نوع من التطبيقات (الكهرومغناطيسية، الكهربائية، الكهروميكانيكية، الخ).

تتصل كل من قوارئ البصمة والأقفال بوحدات التحكم مما يسمح بالتحكم والسيطرة على المناطق المقيدة وكذلك ابواب الراكات والتي تحوي معدات تخزين البيانات.

في حين يعمل البرنامج على تسجيل جميع العمليات لمراجعتها في المستقبل في حالة حدوث أي انتهاك، وهذا يقي من الوقوع في المخاطر والتحقيق في الأحداث التي تتم على النظام.



❖ أمن البيانات الضخمة

هنالك حلول عدة لأمن البيانات الضخمة، من أهمها:

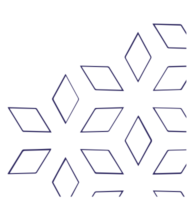
قابلية التوسع تقتضي طبيعة بيئات البيانات الضخمة الاستخدام المتواصل والتوسع المستمر وزيادة حجمها، لهذا يجب أن تكون الحلول الأمنية قادرة على التوسع scalability لتشمل أي زيادة في الحجم من دون التأثير في الأداء.

استمرارية الأداء نظراً لتوفر حلول الذكاء الاصطناعي وتعلم الآلة في العديد من البرمجيات من جانب، ومن جانب آخر الأخطاء البشرية المتوقعة والمتواردة، لذا وجب على أنظمة تحليل البيانات أن تكون ذكية ودقيقة بالقدر الكافي دون الحاجة لتدخل أي عنصر بشري. لذا، من المهم تأمين البيانات الضخمة مزايا الذكاء الاصطناعي دون انقطاع.

الإتاحة والتكيف يجب على الحلول الأمنية ألا تغفل عنصري الإتاحة والتكيف availability and adaptability ولتحقيق أكبر قيمة وحماية، تحتاج هذه الحلول لأن تكون قادرة على الوصول الكامل للبيانات أياً كان مكانها في المؤسسة أو الجهة المعنية.

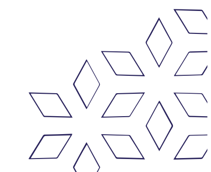
المرونة تستخدم بعض المؤسسات أطر عمل مفتوحة المصدر للبيانات الضخمة مثل Spark، لكن هذه البيئات تعمل على أنظمة قديمة، لذلك من المهم أن تتمتع حلول تأمين البيانات الضخمة بالمرونة الكافية flexiblity لمواكبة التحديثات المتتابعة في مجال البيانات.

تغطية جميع البيئات معظم التطبيقات المستخدمة أصبحت مُستضافة في السحابة cloud-based ، كما أصبحت مصدرا مهما لتخزين البيانات، لذا يجب أن تكون حلول تأمين البيانات قادرة على تأمين الأنظمة الرقمية والبيانات بمختلف أنواعها: المستضافة سحابياً، والمستضافة في بيئة داخل المؤسسات الحكومية، وكذلك الهجين.



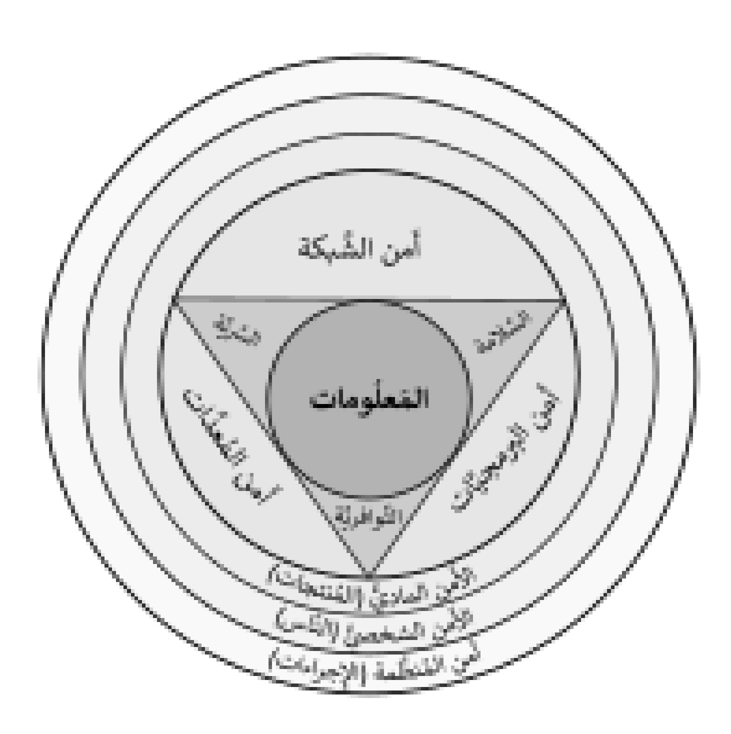
الترميز وهو يعني عملية الاستعاضة عن عناصر حساسة في البيانات بعناصر أخرى tokenization ، وهي خاصية مهمة ستساعد إن توفرت على تأمين بيانات المؤسسة لسنوات طويلة مقبلة، واستبعاد المخاوف المتعلقة بالخصوصية.

وأخيرا، فإن البيانات الضخمة تشكل طفرة كبيرة في عالم التقنية والاقتصاد، ولكنها في الوقت نفسه تنطوي على العديد من المخاطر للمستخدم ولاسيما ما يتعلق بالخصوصية، إن البيانات الضخمة والأدوات المرتبطة بها تعزز سطوة المؤسسات الكبرى على تفاصيل حياة الأفراد مما يهدد بتزايد الاعتداء على الحريات الفردية ومن ثم تقويض الأنظمة الاجتماعية، لذلك، ودون الوقوع في فخ التهويل والمبالغة، يجب تعزيز الوعي لدى المستخدمين بمخاطر هذه التقنيات بحيث تستخدم بحذر، كذلك يجب على المؤسسات الممثّلة للشعوب أن تعمل على تعزيز البيئة القانونية والتنظيمية التي من شأنها حماية مصالح المواطنين وحرياتهم.

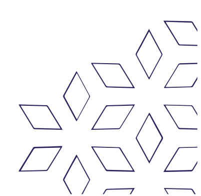


❖ أمن الهواتف النقالة

أمن الهواتف الذكية أصبح أمن الهواتف ذا أهمية كبيرة، وذلك بسبب التوسع في انتشار الهواتف النقالة (الذكية)، ومما يثير القلق بشكل خاص هو أمن المعلومات الشخصية والتجارية المخزنة الآن على الهواتف الذكية، كما أن الكثير من مستخدمي الإنترنت يستخدمون الهواتف الذكية مثل وسائل الاتصال، أيضاً كوسيلة لتخطيط وتنظيم عملهم وحياتهم الخاصة، الهواتف الذكية تحتوي على كمية كبيرة من المعلومات الحساسة التي يجب الحفاظ عليها وحمايتها، كما يجب معرفة أن جميع الهواتف الذكية، وأجهزة الحاسوب هي الأهداف المفضلة للهجمات، وهذه الهجمات غالباً ما تستغل نقاط الضعف المتعلقة بالهواتف الذكية التي يمكن أن تأتي من وسائل الاتصال مثل خدمة الرسائل القصيرة SMS، وخدمة الرسائل متعددة الوسائط MMS، وجي اس ام GSM وشبكات الواي فاي Wi-Fi.



امن المعلومات

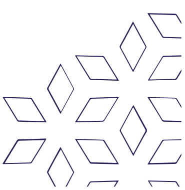


❖ المواطنة الرقمية

المواطنة الرقمية هي مجموع القواعد والضوابط والمعايير والأعراف والأفكار والمبادئ المتبعة في الاستخدام الأمثل والقويم للتكنولوجيا، والتي يحتاجها المواطنون صغارا وكبارا من أجل المساهمة في رقي الوطن، المواطنة الرقمية باختصار هي توجيه وحماية، توجيه نحو منافع التقنيات الحديثة، وحماية من أخطارها، أو باختصار أكبر هي التعامل الذكي مع التكنولوجيا.

لا ينبغي أن نفهم من معنى المواطنة الرقمية أنها تهدف إلى نصب الحدود والعراقيل من أجل التحكم والمراقبة، بمعنى التحكم من أجل التحكم، الشيء الذي يصل أحيانا إلى القمع والاستبداد ضد المستخدمين بما يتنافى مع قيم الحرية والعدالة الاجتماعية وحقوق الإنسان، فالمواطنة الرقمية إنما تهدف إلى إيجاد الطريق الصحيح لتوجيه وحماية جميع المستخدمين خصوصا منهم الأطفال والمراهقين، وذلك بتشجيع السلوكات المرغوبة ومحاربة السلوكات المنبوذة في التعاملات الرقمية، من أجل مواطن رقمي يحب وطنه ويجتهد من أجل تقدمه.

يمكن تعريف المواطنة الرقمية كذلك بأنها قواعد السلوك المعتمدة في استخدامات التكنولوجيا المتعددة، مثل استخدامها من أجل التبادل الإلكتروني للمعلومات، والمشاركة الإلكترونية الكاملة فى المجتمع، وشراء وبيع البضائع عن طريق الإنترنت، وغير ذلك، وتعرف أيضا بأنها القدرة على المشاركة فى المجتمع عبر شبكة الإنترنت، كما أن المواطن الرقمي هو المواطن الذي يستخدم الإنترنت بشكل منتظم وفعال.



❖ الأمن الرقمي

يشير مصطلح" الأمان الرقمي" أو "الأمن الرقمي "إلى كل تلك الطرق المختلفة والمتعددة التي تكون غايتها هي حماية حسابات الإنترنت المتعلقة في الحاسب الآلي وحماية الملفات من التسلل أو التدخل والتطفل من قبل مستخدمين خارجيين (غير مصرحين).

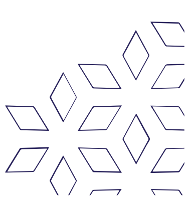
أهمية الامن الرقمي

زادت انتهاكات أمن البيانات بشكلٍ هائل في العقد الماضي، حيث تعرّض أكثر من سبعة ملايين سجل بيانات إلى الاختراق بشكل يومي، كما زادت نسبة الاحتيال الإلكتروني، وسوء استخدام الانترنت بشكل ملاحظ، إذ أنّ مجرمي الانترنت، يعمدون إلى استغلال قيمة ونوع البيانات المختلفة، في تحقيق مرادهم، **ومن هنا تأتي أهميّة الامن الرقمي في حماية هذه البيانات المعرّضة للخطر :**

- **بيانات التعريف الشخصيّة:** وهي تتضمّن الاسم والبريد الإلكتروني والعنوان، ورقم الضمان الاجتماعي الذي يعدّ الأكثر خطراً، حيث يمكن استخدام رقم الضمان الاجتماعي من قبل المُخترق، لفتح حساب بطاقة ائتمان باسم الشخص.
- **بيانات الدفع الشخصيّة:** وهي تشمل أرقام بطاقات الائتمان، وأرقام الخدمات المصرفيّة، وأكواد PIN والتي يمكن لمجرمي الانترنت استخدامها، لتحويل الأموال من حسابك المصرفي، أو لإجراء عمليات شراء.
- **بيانات الصحة الشخصيّة:** ويقصد بها المعلومات الصحيّة، والأدوية الموصوفة للشخص، والتأمين الصحي، والزيارات إلى الأطباء أو المشافي، وهي معلومات هامة جداً، لمجرمي الانترنت الذين يستغلّون هذه المعلومات الصحيّة للمطالبة بالتأمين الصحي، أو طلب أدوية وإعادة بيعها.

ما الفرق بين الامن الرقمي والأمن السيبراني

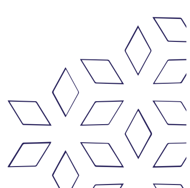
بشكل عام، تخلق الحاجة إلى الامن الرقمي والأمن السيبراني عند حدوث الجرائم الالكترونية، كانتهاك بيانات شخص ما، مع ذلك هناك فرق بين الأمن القومي والأمن السيبراني، فالأمن القومي يضمن حماية تواجد الأشخاص على الانترنت، من خلال حماية بياناتهم وهويتهم وأصولهم، في حين يحمي الأمن السيبراني جميع الشبكات، وأنظمة كمبيوتر، والمعلومات من الاختراق، وبذلك يمكن اعتبار الأمن الرقمي جزءاً من الأمن السيبراني.



❖ الاتصالات الرقمية

الاتصالات الرقمية هي الاتصالات التي تتعامل بمبدأ النظام الثنائي، يتصف هذا النوع من الاتصالات بقوتها وجودتها العالية مقارنة بالاتصالات التناظرية؛ حيث إن هناك ما يسمى بالضوضاء الكهرومغناطيسية في الطبيعة، هذه الضوضاء تسبب تشوشاً في الإشارة التناظرية التي تعتمد على شدة التيار وتردده، لكن في حالة استخدام النظام الثنائي، فإن الإشارات تحسب بمرور نبضة أو عدم مرورها، فلا تتأثر بالتشويش الذي تسببه الضوضاء الكهرومغناطيسية.

من أمثلة الأجهزة التي تعتمد الاتصالات الرقمية: التلفاز الرقمي، اتصالات السواتل، والحواسيب، يشار إلى إن الإشارات الرقمية تنتج من تقطيع الإشارات التناظرية إلى أجزاء كل جزء يمثل هو يمثل مجموعة من ٠ و ١ وتسمى أيضا بتقنية الدجيتال بالإنجليزية (digital) : ويمكن التحويل من النظام الثنائي إلى النظام التناظري عن طريق جهاز يعرف بالمحول الثنائي التناظري، والتحويل من التناظري إلى الثنائي عن طريق المحول التناظري الثنائي، أما عن طريقة التحويل من كلا النظامين إلى الآخر دون استخدام أجهزة التحويل سالفة الذكر باستخدام طريقة التحويل اليدوية فقد استخدمت هذه الطرق في التعليم وفي التطبيق العملي للتحويل حال عدم وجود هذه الأجهزة، فعن الطريقة تحويل من النظام الثنائي إلى عشري كالتالي: تحويل ١,١,٠,٠,١ من النظام الثنائي إلى العشري يتم وضع قيمة صغرى فوق العدد بدأ من صفر وانتهاء بعشرة: فقيمة الرقم ١= ٠ و ١=٠ و ٢=٠ و ٣=١ و ٤=١ ويتم جمع الأعداد التي لها قيمة (أي تملك الرقم (١) فينتج من النظام الثنائي ١,١,٠,٠,١ العدد العشري ٧ وللتحويل من النظام العشري إلى الثنائي نقسم العدد على (٢) فإذا كان هناك باقي للقسمة نعطي الرقم ١ وإلى ٠ كالتالي: تحويل الرقم ٧ من النظام العشري إلى الثنائي: بتقسيم العدد ٧ على ٢ ينتج ٣ والباقى ١ وبتقسيم العدد ٣ على ٢ ينتج ١ والباقي ١ وهكذا حتى ينتج ١,١,١.

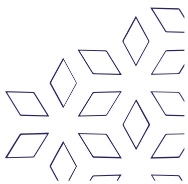


مزايا الاتصالات الرقمية

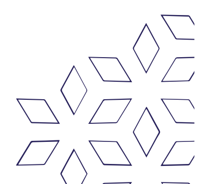
تنبع الميزة الكبرى لاستخدام أنظمة الاتصالات الرقمية من قدرة جهاز الاستقبال على التعامل مع البيانات المستقبلة على أنها «أرقام» وإخضاعها لعمليات حسابية يمكن من خلالها الحصول على فوائد متعددة. وهذا بالمقارنة بالاتصالات التناظرية التي يكون فيها «شكل» الإشارة المستقبلة هو المحتوي على المعلومة، وبالتالي فإن أي تغير في الشكل نتيجة إضافة الضوضاء (الشوشرة) في قناة الاتصال سوف يتحول على الفور إلى فقد أو تشوه في المعلومات التي تحملها هذه الإشارة، مثل تغير في جودة الصوت أو الصورة أو الفيديو الذي تحمله الإشارة.

على وجه التحديد، يمكن إيجاز مزايا الاتصالات الرقمية فيما يلي:

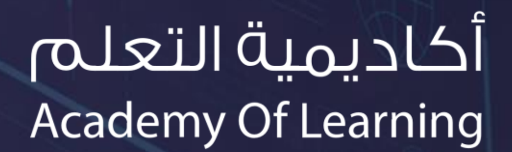
- القدرة على استخدام «المعيدات التي تعيد توليد الإشارة» والتي تعرف باللغة الإنجليزية باسم "Regenerative Repeaters". إذ أن الإشارة الرقمية، حتى وإن تعرضت لنسبة معينة من الشوشرة، يمكن أن تفهمها أجهزة الاستقبال بطريقة صحيحة، وتعيد تشكيلها في صورتها الأصلية، مما يجعل الإشارات الرقمية تعطي نتائج فائقة الجودة والدقة.
- سهولة تطبيق أنظمة الترميز للتحكم في الخطأ ("Error Control Coding") وتتمثل الفكرة العامة لها في استغلال المدلولات الرقمية للإشارة في عمليات حسابية مبسطة، تلحق نتائجها بالإشارة الرقمية، وفي جهاز الاستقبال، يتم إجراء نفس العمليات الحسابية على المدلولات الرقمية المستقبلة، ومقارنة النتائج المتحصل عليها بالنتائج المستقبلة للتحقق من عدم وجود خطأ، وتستطيع هذه النظم أن تصحح الخطأ في ظروف معينة، ويعرف هذا النوع بالنظم الأمامية لتصحيح الخطأ("Forward Error Correction") ، في إشارة إلى عدم طلب إعادة الإرسال من جهاز الإرسال وتوجد نظم أخرى تعتمد على اكتشاف الخطأ في جهاز الاستقبال، ثم طلب إعادة الإرسال أوتوماتيكيًا من المُرسِل فيما يعرف باسم أنظمة طلب التكرار آليًا ("Automatic Repeat Request") وتعرف اختصاراً بأنظمة ARQ.



- إمكانية تطبيق أنظمة التشفير، ("Ciphering/Encryption") وهي تعتمد بنفس الطريقة على تحويل المدلولات الرقمية في الإشارة إلى مدلولات أخرى تبدو للمستقبل كما لو كانت عشوائية (لا تحتوي على معلومات) وبالتالي لايمكن فهم معناها إلا بإجراء العمليات الحسابية العكسية، ولا يتاح ذلك إلا لمن يمتلك المفتاح الشفري.
- إمكانية الضغط والتخزين ("Storage and Compression")، حيث يمكن تخزين هذه الإشارات في صورة مدلولات رقمية في ذاكرة مثل ذاكرة الحاسوب، أو ضغطها لتشغل مكانًا أقل في الذاكرة، أو لتستغرق وقتًا أقل عند الإرسال، ومن أمثلة الصيغ الشائعة للملفات الصوتية المضغوطة صيغة mp3 وكذلك، بالنسبة لملفات الصورة صيغة jpg ولملفات الفيديو صيغة mp4.







تحت إشراف



المؤسسة العامة للتدريب التقني والمهني
Technical and Vocational Training Corporation

9 2 0 0 0 3 1 3 7

a o l . e d u . s a

a o l k s a